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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
08 June 2023 (08.06.2023)

WIPO | PCT

(10) International Publication Number
WO 2023/098972 A1

(51) International Patent Classification:
H04L 9/00 (2022.01) *H04L 61/2539* (2022.01)
H04L 9/40 (2022.01) *H04L 101/668* (2022.01)

(21) International Application Number:
PCT/EP2021/083527

(22) International Filing Date:
30 November 2021 (30.11.2021)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant: **HUAWEI TECHNOLOGIES CO., LTD.** [CN/CN]; Huawei Administration Building Bantian, Longgang District, Shenzhen, Guangdong 518129 (CN).

(72) Inventor; and

(71) Applicant *(for MN only)*: **IANNONE, Luigi** [IT/DE]; Huawei Technologies Duesseldorf GmbH, Riesstr. 25, 80992 Munich (DE).

(72) Inventors: **FRESSANCOURT, Antoine**; Huawei Technologies Duesseldorf GmbH, Riesstr. 25, 80992 Munich (DE). **LOU, Zhe**; Huawei Technologies Duesseldorf GmbH, Riesstr. 25, 80992 Munich (DE).

(74) Agent: **KREUZ, Georg M.**; Huawei Technologies Duesseldorf GmbH, Riesstr. 25, 80992 Munich (DE).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, IT, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW.

WO 2023/098972 A1

(54) **Title:** DEVICES AND METHODS FOR ISP-ASSISTED IP ADDRESS PRIVACY PROTECTION

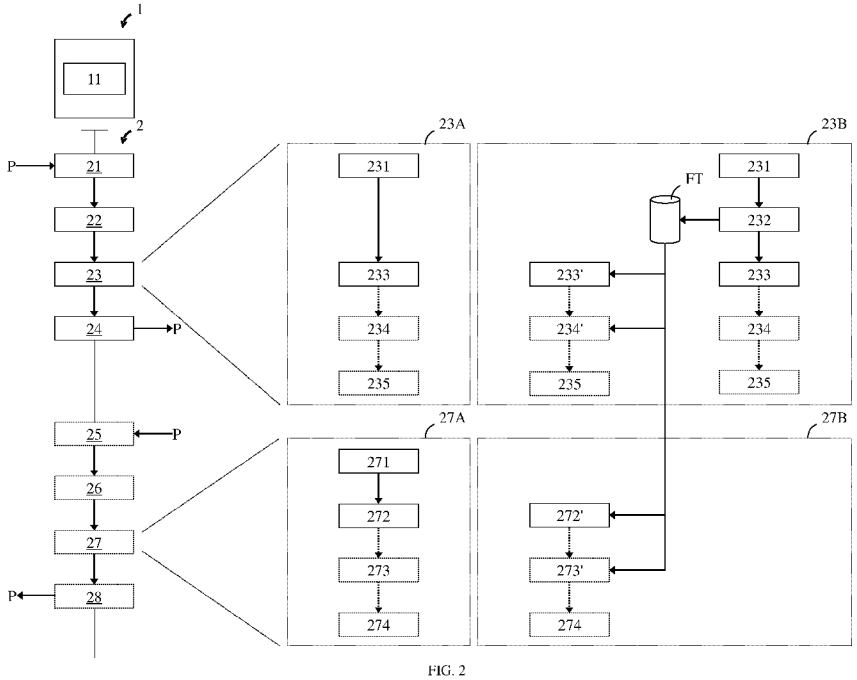

FIG. 2

(57) **Abstract:** Disclosed is a router (1) comprising a processor (11). The processor (11) is configured to: receive (21) a packet (P), wherein a source address of the received packet (P) identifies a first network (F) comprising the router (1), and a destination address of the received packet (P) identifies a second network (S) different from the first network (F); establish (22) if the source address requires obfuscation via encryption; encrypt (23) the source address, if the source address requires obfuscation via encryption; and forward (24) the received packet (P) including the encrypted source address in accordance with the destination address. This protects a privacy of end-user network addresses.

[Continued on next page]

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report (Art. 21(3))*

— *in black and white; the international application as filed contained color or greyscale and is available for download from PATENTSCOPE*

DEVICES AND METHODS FOR ISP-ASSISTED IP ADDRESS PRIVACY PROTECTION

Technical Field

The present disclosure relates generally to the field of network routing, and more particularly to devices and methods for ISP-assisted IP address privacy protection.

Background

IP addresses are considered personal data and as such might be subject to privacy laws, such as the General Data Protection Regulation (GDPR) in Europe. However, IP addresses are sent in clear across the Internet. As such, any observer along the path can read and use them for various tracking purposes. Besides basic information about the network or the device, it is possible to associate an IP address to an end-user – hence the relevance of IP addresses for users' privacy.

General security/privacy solutions aim at protecting all privacy aspects of an IP communication, e.g., end-user and server IP addresses, transport protocol, application communicating, etc. As such, IP address privacy is obtained as a by-product of a more general privacy framework. Some approaches propose to completely revise the current Internet architecture, the routing, and the addressing in the aim to preserve privacy and confidentiality. Furthermore, such kind of approaches ensure the authenticity and correctness of topology propagation and route computation. Some other approaches propose creating a multi-encryption application overlay on the existing Internet architecture. The result is certainly a robust solution security and privacy wise but at the cost of a large overhead, high latency and complex key distribution. Further, Virtual Private Networks (VPNs) are able to provide similar privacy levels but without additional control plane and in addition hiding the end-user IP address. However, it relies on additional software to be installed on the end-user's device, and the lack of control plane makes VPN rather static and, hence, fragile in mobile scenarios.

IP address specific approaches specifically protect only end-user IP address privacy. This means that any other aspects of the communication, such as server IP address, transport protocol, content of the communication, etc. are not protected in any way, and left to be protected through other means. The

most used mechanism to protect privacy at network layer is the use of NAT, which originally has been designed as a transition mechanism rather than as a privacy protection mechanism. Besides, because of the stateful nature of NAT, scalability issues may arise.

As already mentioned, deployment of privacy preserving solutions on the end-user device itself is not desirable, first because of the scale, with billions of devices to be updated, but more importantly because of the risk of breaking the way applications work and network operate. Applications make a number of assumptions about the way the device obtains and uses network addresses, based on current practices, hence any change on those assumptions may break the application.

On the flip side, any mechanism using addresses differently from what the network expects may create trouble in the network itself. If the privacy solution needs any kind of support from the network, which is very likely since devices cannot freely decide their own address but need to respect some local constraints (e.g., the prefix to use), the risk is that the end-user will experience a lack of connectivity.

One last point to consider is about scalability. Because conventional approaches are usually based on some form of state kept on different network elements, the scalability may be limited due to the limited amount of memory available on such network devices.

These limitations highlight the need to allow two parties to exchange information while protecting the digital identity of the end-user. The Internet service does not need privacy protection because usually it is willing to be known, and because it is not a physical person, hence privacy laws usually do not apply.

Summary

These and other limitations are overcome by the features of the independent claims. Further implementation forms are apparent from the dependent claims, the description and the figures.

To protect the privacy of end-users, their IP addresses should not be "public" beyond the local connection.

As such, a mechanism is needed, somewhere in the path between the end-user and the Internet services (e.g., Web or Cloud services), which will take care to obfuscate the IP address of the end-user. The further away from the end-user such privacy service is placed the more exposed the IP address is because of the number of links to be traversed. Furthermore, because of the inherent asymmetry of Internet paths, it becomes more difficult to make both forward and backward packets of the same flow go through the same node, hence requiring state sharing and synchronization among different network elements and/or modification of the routing policies and/or addressing, up to the introduction of topology constraints.

In light of this, the disclosed privacy protection relies on a small operational modification on first hop access routers, which may simply be implemented in software and which does not rely on layers beyond IP and does not require general deployment. As such, the present disclosure leverages on the trust relationship that exists between end-users and their service provider, the latter taking care to prevent the disclosure of users' IP address during the data transmission beyond the local ISP domain. Privacy protection of end-users is achieved by offering an in-network service using cryptographic operations that hide the IP address of end-users with little impact on the forwarding performance and no impact on usual network operation/management/traffic engineering practices of an Internet Service Provider (ISP).

According to a first aspect, a router is provided. The router comprises a processor configured to: receive a packet, wherein a source address of the received packet identifies a first network comprising the router, and a destination address of the received packet identifies a second network different from the first network; establish if the source address requires obfuscation via encryption; encrypt the source address, if the source address requires obfuscation via encryption; and forward the received packet including the encrypted source address in accordance with the destination address.

In other words, an originator of a communication sends a packet with untouched header to an edge router facing end-users (typically the first-hop router) which will cryptographically obfuscate the

originator's source address and forward the packet toward the intended Internet service (i.e., the destination). Such a privacy protection may be also deployed as an edge service in the context of mobile cellular networks.

Advantageously, this privacy protection approach provides cryptographically generated addresses enabling address privacy and flow unlinkability, and at the same time

- does not need end-users' device modification.
- is compatible with current network address configuration methods.
- does not need network-wide support in the ISP (single router in front of the user is sufficient).
- does not have scalability limits when implementing a stateless mode of operation.
- provides adaptive privacy granularity.
- may prevent flow correlation (two flows between same source and destination should not be correlated).
- is incrementally deployable meaning that it is not necessary to have support from both communicating parties and early adopters have full benefits without needing other parties to deploy the solution.
- is transparent to other network elements. Once deployed the privacy protection is completely transparent to the communicating parties (end-user and Internet Service), except for some additional small latency due to the cryptographic operations.
- is GDPR compliant.
- does not share cryptographic material among several entities, as it remains local to the router providing the privacy service.

Where latency is an issue, a stateful mode of operation can be used (at the cost of scalability).

If not all traffic of end-users has to be encrypted it is easy to indicate the need for user privacy via dedicated prefixes (e.g., end-user uses two prefixes, one to be privacy protected the other public) or via explicit signalling (e.g., DSCP). Signal free solutions by which the end-user just uses any existing NAT-traversal mechanism can also be implemented.

In a possible implementation form, the processor may further be configured to establish that the source address requires obfuscation via encryption upon one of: a source prefix of the source address matching a user privacy prefix; the source prefix comprising a user privacy indication; a header of the received packet comprising a user privacy indication; and unconditional encryption of any received packet.

Advantageously, the need for end-user privacy may be indicated in a number of ways in a stateless mode of operation involving a cryptographic operation for each packet of a flow of packets.

In a possible implementation form, the processor may further be configured to establish that the source address requires obfuscation via encryption upon: the source address and the destination address of the received packet matching a source address and a destination address of an entry of a flow table of the router, respectively.

Advantageously, the need for end-user privacy may be indicated also in a stateful mode of operation involving a cryptographic operation for each first packet of a flow of packets and a flow table lookup for each subsequent packet of the flow of packets.

In a possible implementation form, the processor may further be configured to: receive a packet, wherein a destination prefix of a destination address of the received packet identifies the first network comprising the router, and a source prefix of a source address of the received packet identifies the second network different from the first network; establish if the destination address requires decryption; decrypt the destination address, if the destination address requires decryption; and forward the received packet including the decrypted destination address in accordance with the decrypted destination address.

Advantageously, packets from the prompted Internet service to the originator will go through the same privacy service which will reinstate the address of the originator and forward the packet to it.

In a possible implementation form, the processor may further be configured to establish that the destination address requires decryption upon one of: a destination prefix of the destination address

matching the user privacy prefix; the destination prefix matching a network privacy prefix; and unconditional decryption of any received packet.

Advantageously, the need for reinstatement of the address of the originator may be established in a number of ways in a stateless mode of operation.

In a possible implementation form, the processor may further be configured to establish that the destination address requires decryption upon: the source address and the destination address of the received packet matching the destination address and the encrypted source address of an entry of the flow table of the router, respectively.

Advantageously, the need for reinstatement of the address of the originator may also be established in a stateful mode of operation.

In a possible implementation form, the processor may further be configured to, so as to encrypt the source address: encrypt a first data set using a first cryptographic key, the first data set comprising a source suffix of the source address.

Advantageously, the address of the originator, in particular its suffix, may be concealed in both a stateless mode of operation and a stateful mode of operation.

In a possible implementation form, the first data set may further comprise one or more of: a source port number of the received packet; a random variable; a prefix alignment for compensation of a difference in size of the user privacy prefix and the network privacy prefix; and a version of the first cryptographic key.

Advantageously, the port number of the originator may also be concealed, and further elements may be included in the concealment for increasing randomness (a nonce, i.e., the random variable), for size compensation (the prefix alignment comprising a number of '0' hexadecimal (hex) values) or and/or key rolling (the key's version no.).

In a possible implementation form, the processor may further be configured to, so as to encrypt the source address: replace the source suffix of the received packet by the encrypted source suffix derived from the encrypted first data set.

Advantageously, the source suffix may be concealed for all packets in a stateless mode of operation, and for a first packet in a stateful mode of operation.

In a possible implementation form, the processor may further be configured to, so as to encrypt the source address: replace the source port number of the received packet by an encrypted source port number derived from the encrypted first data set.

Advantageously, the source port number may be concealed in all packets of a flow in a stateless mode of operation, and for a first packet of a flow in a stateful mode of operation.

In a possible implementation form, the populated entry of the flow table may further comprise the encrypted source port number.

Advantageously, the source port number may be concealed in subsequent packets of a flow in a stateful mode of operation.

In a possible implementation form, the processor may further be configured to, so as to encrypt the source address: populate the flow table with an entry comprising the source address of the received packet, the destination address of the received packet, and an encrypted source address comprising the encrypted source suffix.

Advantageously, a stateful mode of operation may be supported by a NAT-like flow table.

In a possible implementation form, the processor may further be configured to, so as to encrypt the source address: replace the source suffix of the received packet by the encrypted source suffix of the matching entry of the flow table.

Advantageously, the source suffix may be concealed for subsequent packets in a stateful mode of operation.

In a possible implementation form, the processor may further be configured to, so as to encrypt the source address: replace the source port number of the received packet by the encrypted source port number of the matching entry of the flow table.

Advantageously, the source port number may be concealed for subsequent packets in a stateful mode of operation.

In a possible implementation form, the processor may further be configured to, so as to encrypt the source address: replace the source prefix of the received packet by the network privacy prefix.

Advantageously, the source prefix, for instance the user privacy prefix, may be concealed by the network privacy prefix for subsequent packets in a stateful mode of operation.

In a possible implementation form, the processor may further be configured to, so as to decrypt the destination address: decrypt a second data set using a second cryptographic key, the second cryptographic key being suitable for cancelling an encryption by the first cryptographic key, the second data set comprising a destination suffix of the destination address.

Advantageously, a concealment of the address of the originator, in particular its suffix, may be cancelled in a stateless mode of operation.

In a possible implementation form, the second data set may further comprise a destination port number of the received packet.

Advantageously, a concealment of the destination port number may also be cancelled in a stateless mode of operation.

In a possible implementation form, the processor may further be configured to, so as to decrypt the destination address: replace the destination suffix of the received packet by a destination suffix derived from the decrypted second data set.

Advantageously, a concealment of the destination suffix may be cancelled in a stateless mode of operation.

In a possible implementation form, the processor may further be configured to, so as to decrypt the destination address: replace the destination port number of the received packet by the destination port number derived from the decrypted second data set.

Advantageously, a concealment of the destination port number may be cancelled in a stateless mode of operation.

In a possible implementation form, the processor may further be configured to, so as to decrypt the destination address: replace the destination prefix of the received packet by the user privacy prefix.

Advantageously, a concealment of the user privacy prefix by the network privacy prefix may be cancelled in both a stateless mode of operation and in a stateful mode of operation.

In a possible implementation form, the processor may further be configured to, so as to decrypt the destination address: replace the destination suffix of the received packet by the source suffix of the matching entry of the flow table.

Advantageously, a concealment of the destination suffix may also be cancelled in a stateful mode of operation.

In a possible implementation form, the processor may further be configured to, so as to decrypt the destination address: replace the destination port number of the received packet by the source port number of the matching entry of the flow table.

Advantageously, a concealment of the destination port number may also be cancelled in a stateful mode of operation.

In a possible implementation form, the first cryptographic key and the second cryptographic key may comprise a same symmetric cryptographic key.

Advantageously, known symmetric cryptography may be used.

In a possible implementation form, the first cryptographic key may comprise a public key of an asymmetric cryptographic key pair; and the second cryptographic key may comprise a private key of the asymmetric cryptographic key pair.

Advantageously, known asymmetric cryptography may be deployed.

According to a second aspect, a method of operating a router is provided. The method comprises: receiving a packet, wherein a source address of the received packet identifies a first network comprising the router, and a destination address of the received packet identifies a second network different from the first network; establishing if the source address requires obfuscation via encryption; encrypting the source address, if the source address requires obfuscation via encryption; and forwarding the received packet including the encrypted source address in accordance with the destination address.

Advantageously, the technical effects and advantages described above in relation with the router equally apply to the method of operating said router having corresponding features.

Brief Description of Drawings

The above-described aspects and implementations will now be explained with reference to the accompanying drawings, in which the same or similar reference numerals designate the same or similar elements.

The drawings are to be regarded as being schematic representations, and elements illustrated in the drawings are not necessarily shown to scale. Rather, the various elements are represented such that their function and general purpose become apparent to those skilled in the art.

FIG. 1 illustrates an exemplary network scenario in accordance with the present disclosure; and

FIG. 2 illustrates a router and a method of operating the same, both in accordance with the present disclosure;

Detailed Description

In the following description, reference is made to the accompanying drawings, which form part of the disclosure, and which show, by way of illustration, specific aspects of implementations of the present disclosure or specific aspects in which implementations of the present disclosure may be used. It is understood that implementations of the present disclosure may be used in other aspects and comprise structural or logical changes not depicted in the figures. The following detailed description, therefore, is not to be taken in a limiting sense, and the scope of this disclosure is defined by the appended claims.

For instance, it is understood that a disclosure in connection with a described method may also hold true for a corresponding apparatus or system configured to perform the method and vice versa. For example, if one or a plurality of specific method steps are described, a corresponding device may include one or a plurality of units, e.g. functional units, to perform the described one or plurality of method steps (e.g. one unit performing the one or plurality of steps, or a plurality of units each performing one or more of the plurality of steps), even if such one or more units are not explicitly described or illustrated in the figures. On the other hand, for example, if a specific apparatus is described based on one or a plurality of units, e.g. functional units, a corresponding method may

include one step to perform the functionality of the one or plurality of units (e.g. one step performing the functionality of the one or plurality of units, or a plurality of steps each performing the functionality of one or more of the plurality of units), even if such one or plurality of steps are not explicitly described or illustrated in the figures. Further, it is understood that the features of the various exemplary aspects described herein may be combined with each other, unless specifically noted otherwise.

A router or routing device as used herein may generally refer to a network node capable of layer-3 routing. In other words, a network comprising such a router may be a routed network, such as an IP network.

A packet as used herein may refer to what is known as "datagram", namely a "self-contained, independent entity of data carrying sufficient information to be routed from the source to the destination computer without reliance on earlier exchanges between this source and destination computer and the transporting network" (see RFC 1594).

Encryption and decryption as used herein may refer to the cryptographic operations of encoding plaintext (i.e., unciphered) information, such as bitstrings, into a ciphertext representation (encryption) and decoding encrypted information into the original plaintext (i.e., unciphered) representation (decryption).

An address as used herein may generally refer to a network address of *M* bits length including an address prefix of *N* bits length and an address suffix of *M-N* bits length. Particularly, an address as used herein may refer to an IPv6 network address of *M=128* bits length.

A user public prefix as used herein may refer to an address prefix, in particular an IPv6 address prefix such as 2001:db8:0:0::/64 (i.e., *N=64*), used to indicate a privacy unprotected network address relating to an end-user of an ISP (of note, the fictional example addresses mentioned herein relate to the IPv6 prefix 2001:db8::/32 which is generally allocated for documentation purposes, see RFC 3849).

A user privacy prefix as used herein may refer to an address prefix, in particular an IPv6 address prefix such as 2001:db8:0:ffff::/64 (i.e., *N=64*), used to indicate a (need for a) privacy protected network address relating to an end-user.

A network privacy prefix as used herein may refer to an address prefix, in particular an IPv6 address prefix such as 2001:db8:ffff::/48 (i.e., *N=48*), used to indicate a privacy protected network address relating to an ISP.

A matching as used herein may refer to an operation wherein a match (or accordance, agreement, correspondence, ...) of a plurality of operands is verified (or falsified).

Network address translation (NAT) as used herein may refer to a standardized method (see RFC 3022) of mapping an (IPv4) address space into another (IPv4) address space by modifying network address information in transit across a router.

A flow or packet flow as used herein may refer to a sequence of packets (i.e., datagrams, to be more specific) corresponding to one another in terms of both source address and destination address, respectively.

A flow table as used herein may refer to a NAT-like table wherein information gathered in connection with a first packet of a packet flow may be stored for re-use in connection with subsequent packets of the same packet flow.

A stateless mode of operation may refer to an operating principle wherein all packets of a packet flow are treated equally without a need for the router to maintain any form of state associated with the packet flow.

A stateful mode of operation may refer to an operating principle wherein a first packet of a packet flow sent to an Internet service is treated as elaborately as in the stateless mode of operation to generate state information provided in a flow table. All subsequent packets of the packet flow as well

as all packets of the response packet flow received from the Internet service are treated in accordance with (and benefit from) this state information.

FIG. 1 illustrates an exemplary network scenario in accordance with the present disclosure.

To the left, a plurality of end-users U are indicated. The plurality of end-users U is provided with a broadband Internet service by an Internet Service Provider (ISP) operating a first network F, in particular an IP network.

The disclosed privacy protection is general, but will be described in the context of IPv6 hereinafter. The address configuration of the plurality of end-users U is done by any IPv6 address configuration mechanism, with the exception of Cryptographically Generated Addresses (CGA, see RFC 3972), because CGA aims at IP address authentication, which is the opposite of privacy.

A router 1 (a.k.a. first-hop router, edge router) facing the plurality of end-users U serves as a default gateway to other networks, such as a second network S to the right of FIG. 1 which is reachable via the larger Internet I. An Internet or Web service W is provided / hosted in the second network S.

To protect the privacy of the plurality of end-users U when making use of the service W, their IP addresses should not be "public" beyond the local connection between the respective end-user U and the router 1.

FIG. 2 illustrates a router 1 and a method 2 of operating the same, both in accordance with the present disclosure.

The router 1 comprises a processor 11 (see top-left of FIG. 2). The processor 11 may be configured to execute instructions of a computer program and to thereby perform the method 2 of the second aspect (or any of its implementations) of operating the router 1.

A most generic representation of the method 2 (see left of FIG. 2, indicated by solid lines) comprises steps 21 through 24. More specifically, the method 2 comprises:

- receiving 21 a packet, wherein a source address of the received packet P identifies a first network F comprising the router 1, and a destination address of the received packet P identifies a second network S different from the first network F;
- establishing 22 if the source address requires obfuscation via encryption;
- encrypting 23 the source address, if the source address requires obfuscation via encryption; and
- forwarding 24 the received packet P including the encrypted source address in accordance with the destination address.

The method 2 of the second aspect may be performed by the router 1 of the first aspect or any of its implementations.

Those skilled in the art will readily appreciate that the respective features/steps of the method 2 correspond to respective features of the router 1 and vice versa. Thus, further details of FIG. 2 will merely be explained in relation to the router 1 and its processor 11, respectively.

In respect of traffic sent to an Internet service, the processor 11 is configured to: receive 21 a packet P, wherein a source address of the received packet P identifies a first network F comprising the router 1, and a destination address of the received packet P identifies a second network S different from the first network F.

The processor 11 is further configured to establish 22 if the source address requires obfuscation via encryption.

In a stateless mode of operation, the processor 11 may further be configured to establish 22 *that* the source address requires obfuscation via encryption upon one of: a source prefix of the source address matching a user privacy prefix; the source prefix comprising a user privacy indication; a header of the received packet P comprising a user privacy indication; and unconditional encryption of any received packet P.

In a stateful mode of operation, the processor 11 may further be configured to establish 22 *that* the source address requires obfuscation via encryption upon: the source address and the destination

address of the received packet P matching a source address and a destination address of an entry of a flow table FT of the router 1, respectively.

The processor 11 is further configured to encrypt 23 the source address, if the source address requires obfuscation via encryption.

In a stateless mode of operation (see implementation indicated as 23A), the processor 11 may further be configured to, so as to encrypt 23 the source address:

- encrypt 231 a first data set using a first cryptographic key, wherein the first data set comprises a source suffix of the source address, and may further comprise one or more of: a source port number of the received packet P; a prefix of the source address; a random variable (i.e., nonce); a prefix alignment for compensation of a difference in size of the user privacy prefix and the network privacy prefix; a version of the first cryptographic key (a.k.a. key version bits); and more parameters depending on the specific cryptographic algorithm and the level of anonymity required;
- replace 233 the source suffix of the received packet P by the encrypted source suffix derived from the encrypted first data set;
- replace 234 the source port number of the received packet P by an encrypted source port number derived from the encrypted first data set, if applicable; and
- replace 235 the source prefix of the received packet P by the network privacy prefix, if applicable.

The source prefix can be replaced with a dedicated (network privacy) prefix which is not associated to any physical network but only used for privacy purposes. Such a prefix does not need to be of the same length as the prefix of the originator.

In a stateful mode of operation (see implementation indicated as 23B), the processor 11 may further be configured to, so as to encrypt 23 the source address for a first packet of a packet flow:

- encrypt 231 the first data set using the first cryptographic key, wherein the first data set comprises the source suffix of the source address, and may further comprise one or more of: the source port number of the received packet P; the random variable; the prefix alignment for compensation of

a difference in size of the user privacy prefix and the network privacy prefix; and the version of the first cryptographic key;

- populate 232 the flow table FT with an entry which comprises the source address of the received packet P, the destination address of the received packet P, an encrypted source address comprising the encrypted source suffix, and which may further comprise the encrypted source port number;
- replace 233 the source suffix of the received packet P by the encrypted source suffix derived from the encrypted first data set;
- replace 234 the source port number of the received packet P by an encrypted source port number derived from the encrypted first data set, if applicable; and
- replace 235 the source prefix of the received packet P by the network privacy prefix, if applicable.

The processor 11 may further be configured to, so as to encrypt 23 the source address for subsequent packets of a packet flow:

- replace 233' the source suffix of the received packet P by the encrypted source suffix of the matching entry of the flow table FT;
- replace 234' the source port number of the received packet P by the encrypted source port number of the matching entry of the flow table FT, if applicable, and
- replace 235 the source prefix of the received packet P by the network privacy prefix, if applicable.

The processor 11 is further configured to forward 24 the received packet P including the encrypted source address in accordance with the destination address.

In respect of traffic received from the prompted Internet service, the processor 11 may further be configured to: receive 25 a packet P, wherein a destination prefix of a destination address of the received packet P identifies the first network F comprising the router 1, and a source prefix of a source address of the received packet P identifies the second network S different from the first network F.

The processor 11 may further be configured to: establish 26 if the destination address requires decryption.

In a stateless mode of operation, the processor 11 may further be configured to establish 26 that the destination address requires decryption upon one of: a destination prefix of the destination address matching the user privacy prefix; the destination prefix matching a network privacy prefix; and unconditional decryption of any received packet P.

In a stateful mode of operation, the processor 11 may further be configured to establish 26 that the destination address requires decryption upon: the source address and the destination address of the received packet P matching the destination address and the encrypted source address of an entry of the flow table FT of the router 1, respectively.

The processor 11 may further be configured to: decrypt 27 the destination address, if the destination address requires decryption.

In a stateless mode of operation (see implementation indicated as 27A), the processor 11 may further be configured to, so as to decrypt 27 the destination address for all packets of a return packet flow:

- decrypt 271 a second data set using a second cryptographic key, wherein the second cryptographic key is suitable for cancelling an encryption by the first cryptographic key, wherein the second data set comprises a destination suffix of the destination address and may further comprise a destination port number of the received packet P;
- replace 272 the destination suffix of the received packet P by a destination suffix derived from the decrypted second data set;
- replace 273 the destination port number of the received packet P by the destination port number derived from the decrypted second data set, if applicable; and
- replace 274 the destination prefix of the received packet P by the user privacy prefix, if applicable.

In a stateful mode of operation (see implementation indicated as 27B), the processor 11 may further be configured to, so as to decrypt 27 the destination address for all packets of a return packet flow:

- replace 272' the destination suffix of the received packet P by the source suffix of the matching entry of the flow table FT;

- replace 273' the destination port number of the received packet P by the source port number of the matching entry of the flow table FT, if applicable; and
- replace 274 the destination prefix of the received packet P by the user privacy prefix, if applicable.

The processor 11 may further be configured to: forward 28 the received packet P including the decrypted destination address in accordance with the decrypted destination address.

The first cryptographic key and the second cryptographic key may comprise a same symmetric cryptographic key. Alternatively, the first cryptographic key may comprise a public key of an asymmetric cryptographic key pair; and the second cryptographic key may comprise a private key of the asymmetric cryptographic key pair. However, both the "public" key and the private key are kept private on the router 1 and not shared with anybody else.

As a practical example for the stateless mode of operation, it is assumed that an end-user U initiates a TCP connection by sending a SYN packet as follows:

Packet header (sent by end-user)		
	`2001:db8:0:ffff::/64`	*source prefix (user privacy prefix)*
	`4a04:65a2:4688:1e66`	*source suffix*
	`f8f8`	*source port no.*
	...	

The router 1 will take these elements and create a first data set (i.e., bit string) that will undergo cryptographic operation (for the sake of simplicity, no other elements like for instance a nonce are shown):

Unencrypted bit string ("first data set"):		
	`0000`	*prefix alignment (taking care of different prefix sizes)*
	`4a04:65a2:4688:1e66`	*source suffix*
	`f8f8`	*source port no.*

	0000 0000	*padding (taking care of different sizes of the above bit string elements and the encryption key)*

Such a bit string can for example be fed to the AES (Advanced Encryption Standard) cryptographic algorithm in order to derive a new bit string that basically contains a new suffix and a new port number:

Encryption key		
	2b7e151628aed2a6abf7158809cf4f	*exemplary AES key*

Encrypted bit string		
	50fe:2dc8:fccf:743e:c46f	*encrypted source suffix*
	cf11	*encrypted source port no.*
	9baf ec60	*encrypted padding (not used any further)*

These two elements will be used, along a pre-configured privacy prefix, to replace the corresponding fields in the original packet, namely source address and source port number, and then forwarding the packet according to normal routing.

Packet header		
	2001:db8:ffff::/48	*source prefix (network privacy prefix)*
	50fe:2dc8:fccf:743e:c46f	*encrypted source suffix*
	cf11	*encrypted source port no.*
	...	

In particular, the network privacy prefix provides a larger anonymity set ($2^{128-84} = 2^{80}$) than the user privacy prefix ($2^{128-64} = 2^{64}$).

When packets are received from the web service in response, the same cryptographic algorithm and key is used to recover the real intended destination of the packet (the end-user).

Packet header		
	2001:db8:ffff::/48	*destination prefix (network privacy prefix)*
	50fe:2dc8:fccf:743e:c46f	*encrypted destination suffix*
	cf11	*encrypted destination port no.*
	...	

Undecrypted bit string		
	50fe:2dc8:fccf:743e:c46f	*encrypted source suffix*
	cf11	*encrypted source port no.*
	0000 0000	*padding*

5

Decryption key		
	2b7e151628aed2a6abf7158809cf4f	*exemplary AES key*

Decrypted bit string		
	0000	*decrypted prefix alignment (not used any further)*
	4a04:65a2:4688:1e66	*decrypted destination suffix*
	f8f8	*decrypted destination port no.*
	9baf ec60	*decrypted padding (not used any further)*

Packet header (received by end-user)		
	2001:db8:0:ffff::/64	*destination prefix (user privacy prefix)*
	4a04:65a2:4688:1e66	*destination suffix*
	f8f8	*destination port no.*
	...	

Of note, no state is necessary on the router 1, and the key used for cryptographic operation is not shared with any other network elements outside the edge router.

The present disclosure has been described in conjunction with various aspects as examples as well as implementations. However, other variations can be understood and effected by those persons skilled in the art and practicing the claimed matter, from the studies of the drawings, this disclosure and the independent claims. For example, the blocks in the block sequences 232→233→234→235, 233→234→235, 233'→234'→235, 272→273→274 and 272'→273'→274 (see FIG. 2) may be re-ordered arbitrarily within the respective block sequence. In the claims as well as in the description the word "comprising" does not exclude other elements or steps and the indefinite article "a" or "an" does not exclude a plurality. A single element or other unit may fulfill the functions of several entities or items recited in the claims. The mere fact that certain measures are recited in the mutual different dependent claims does not indicate that a combination of these measures cannot be used in an advantageous implementation. A computer program may be stored/distributed on a suitable medium, such as an optical storage medium or a solid-state medium supplied together with or as part of other hardware, but may also be distributed in other forms, such as via the Internet or other wired or wireless telecommunication systems.

Claims

1. A router (1), comprising

a processor (11), configured to

receive (21) a packet (P), a source address of the received packet (P) identifying a first network (F) comprising the router (1), and a destination address of the received packet (P) identifying a second network (S) different from the first network (F);

establish (22) if the source address requires obfuscation via encryption;

encrypt (23) the source address, if the source address requires obfuscation via encryption; and

forward (24) the received packet (P) including the encrypted source address in accordance with the destination address.

2. The router (1) of claim 1,

the processor (11) further configured to establish (22) that the source address requires obfuscation via encryption upon one of:

- a source prefix of the source address matching a user privacy prefix,
- the source prefix comprising a user privacy indication,
- a header of the received packet (P) comprising a user privacy indication, and
- unconditional encryption of any received packet (P).

3. The router (1) of claim 1,

the processor (11) further configured to establish (22) that the source address requires obfuscation via encryption upon:

- the source address and the destination address of the received packet (P) matching a source address and a destination address of an entry of a flow table (FT) of the router (1), respectively.

4. The router (1) of any one of the claims 1 to 3,

the processor (11) further configured to

receive (25) a packet (P), a destination prefix of a destination address of the received packet (P) identifying the first network (F) comprising the router (1), and a source prefix of a source address of the received packet (P) identifying the second network (S) different from the first network (F);

establish (26) if the destination address requires decryption;

decrypt (27) the destination address, if the destination address requires decryption; and

forward (28) the received packet (P) including the decrypted destination address in accordance with the decrypted destination address.

5. The router (1) of claim 4,

the processor (11) further configured to establish (26) that the destination address requires decryption upon one of:

- a destination prefix of the destination address matching the user privacy prefix,
- the destination prefix matching a network privacy prefix, and
- unconditional decryption of any received packet (P).

6. The router (1) of claim 4,

the processor (11) further configured to establish (26) that the destination address requires decryption upon:

- the source address and the destination address of the received packet (P) matching the destination address and the encrypted source address of an entry of the flow table (FT) of the router (1), respectively.

7. The router (1) of any one of the claims 1 to 6,

the processor (11) further configured to, so as to encrypt (23) the source address:

encrypt (231) a first data set using a first cryptographic key, the first data set comprising a source suffix of the source address.

8. The router (1) of claim 7,

the first data set further comprising one or more of:

- a source port number of the received packet (P), and

- a random variable,
- a prefix alignment for compensation of a difference in size of the user privacy prefix and the network privacy prefix, and
- a version of the first cryptographic key.

9. The router (1) of claim 7 or claim 8,

the processor (11) further configured to, so as to encrypt (23) the source address:

replace (233) the source suffix of the received packet (P) by the encrypted source suffix derived from the encrypted first data set.

10. The router (1) of claim 9,

the processor (11) further configured to, so as to encrypt (23) the source address:

replace (234) the source port number of the received packet (P) by an encrypted source port number derived from the encrypted first data set.

11. The router (1) of claim 10,

the populated entry of the flow table (FT) further comprising the encrypted source port number.

12. The router (1) of any one of the claims 7 to 11,

the processor (11) further configured to, so as to encrypt (23) the source address:

populate (232) the flow table (FT) with an entry comprising the source address of the received packet (P), the destination address of the received packet (P), and an encrypted source address comprising the encrypted source suffix.

13. The router (1) of claim 12,

the processor (11) further configured to, so as to encrypt (23) the source address:

replace (233') the source suffix of the received packet (P) by the encrypted source suffix of the matching entry of the flow table (FT).

14. The router (1) of claim 13,

the processor (11) further configured to, so as to encrypt (23) the source address:

replace (234') the source port number of the received packet (P) by the encrypted source port number of the matching entry of the flow table (FT).

15. The router (1) of any one of the claims 9 to 14,

the processor (11) further configured to, so as to encrypt (23) the source address:

replace (235) the source prefix of the received packet (P) by the network privacy prefix.

16. The router (1) of any one of the claims 4 to 15,

the processor (11) further configured to, so as to decrypt (27) the destination address:

decrypt (271) a second data set using a second cryptographic key, the second cryptographic key being suitable for cancelling an encryption by the first cryptographic key, the second data set comprising a destination suffix of the destination address.

17. The router (1) of claim 16,

the second data set further comprising a destination port number of the received packet (P).

18. The router (1) of claim 16 or claim 17,

the processor (11) further configured to, so as to decrypt (27) the destination address:

replace (272) the destination suffix of the received packet (P) by a destination suffix derived from the decrypted second data set.

19. The router (1) of claim 18,

the processor (11) further configured to, so as to decrypt (27) the destination address:

replace (273) the destination port number of the received packet (P) by the destination port number derived from the decrypted second data set.

20. The router (1) of claim 18 or claim 19,

the processor (11) further configured to, so as to decrypt (27) the destination address:

replace (274) the destination prefix of the received packet (P) by the user privacy prefix.

21. The router (1) of claim 16 or claim 17,

the processor (11) further configured to, so as to decrypt (27) the destination address:

replace (272') the destination suffix of the received packet (P) by the source suffix of the matching entry of the flow table (FT).

22. The router (1) of claim 21,

the processor (11) further configured to, so as to decrypt (27) the destination address:

replace (273') the destination port number of the received packet (P) by the source port number of the matching entry of the flow table (FT).

23. The router (1) of any one of the claims 7 to 22,

the first cryptographic key and the second cryptographic key comprising a same symmetric cryptographic key.

24. The router (1) of any one of the claims 7 to 22,

the first cryptographic key comprising a public key of an asymmetric cryptographic key pair; and

the second cryptographic key comprising a private key of the asymmetric cryptographic key pair.

25. A method (2) of operating a router (1), comprising

receiving (21) a packet, a source address of the received packet (P) identifying a first network (F) comprising the router (1), and a destination address of the received packet (P) identifying a second network (S) different from the first network (F);

establishing (22) if the source address requires obfuscation via encryption;

encrypting (23) the source address, if the source address requires obfuscation via encryption; and

forwarding (24) the received packet (P) including the encrypted source address in accordance with the destination address.

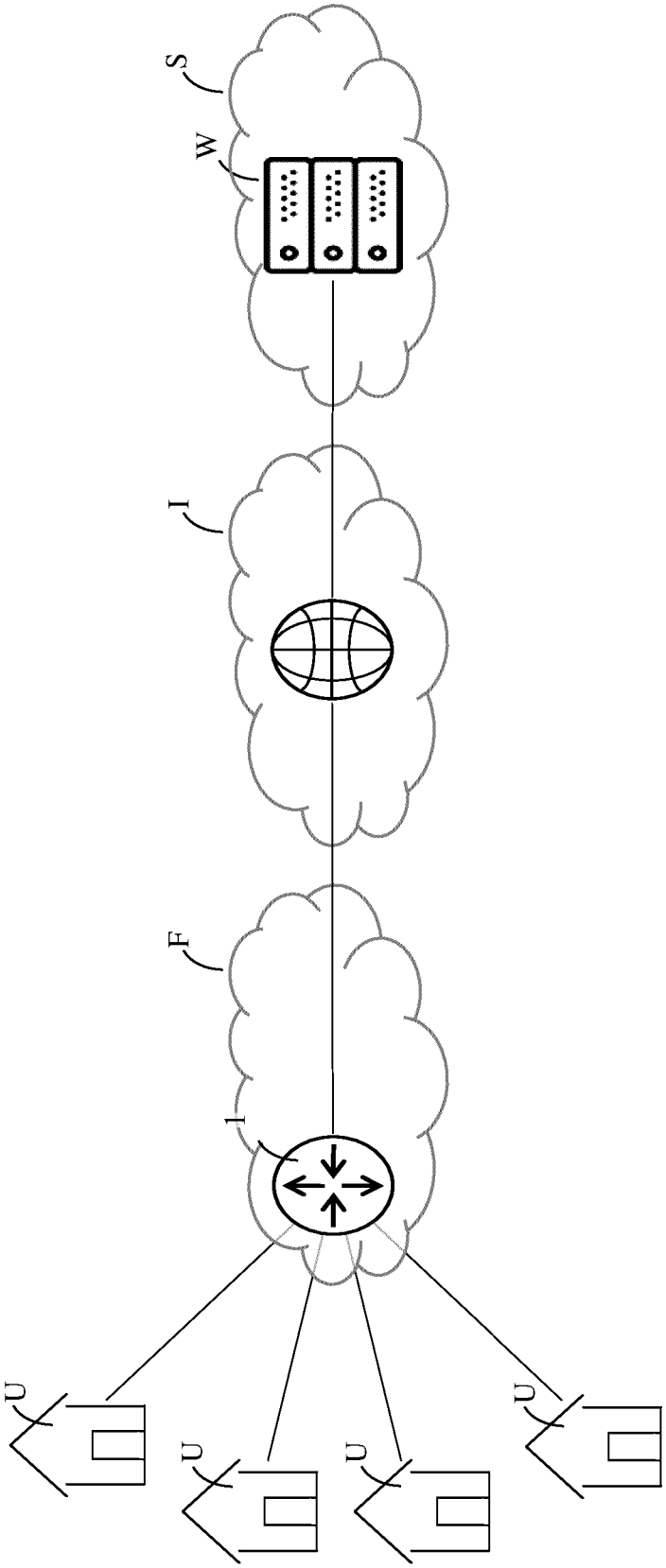

FIG. 1

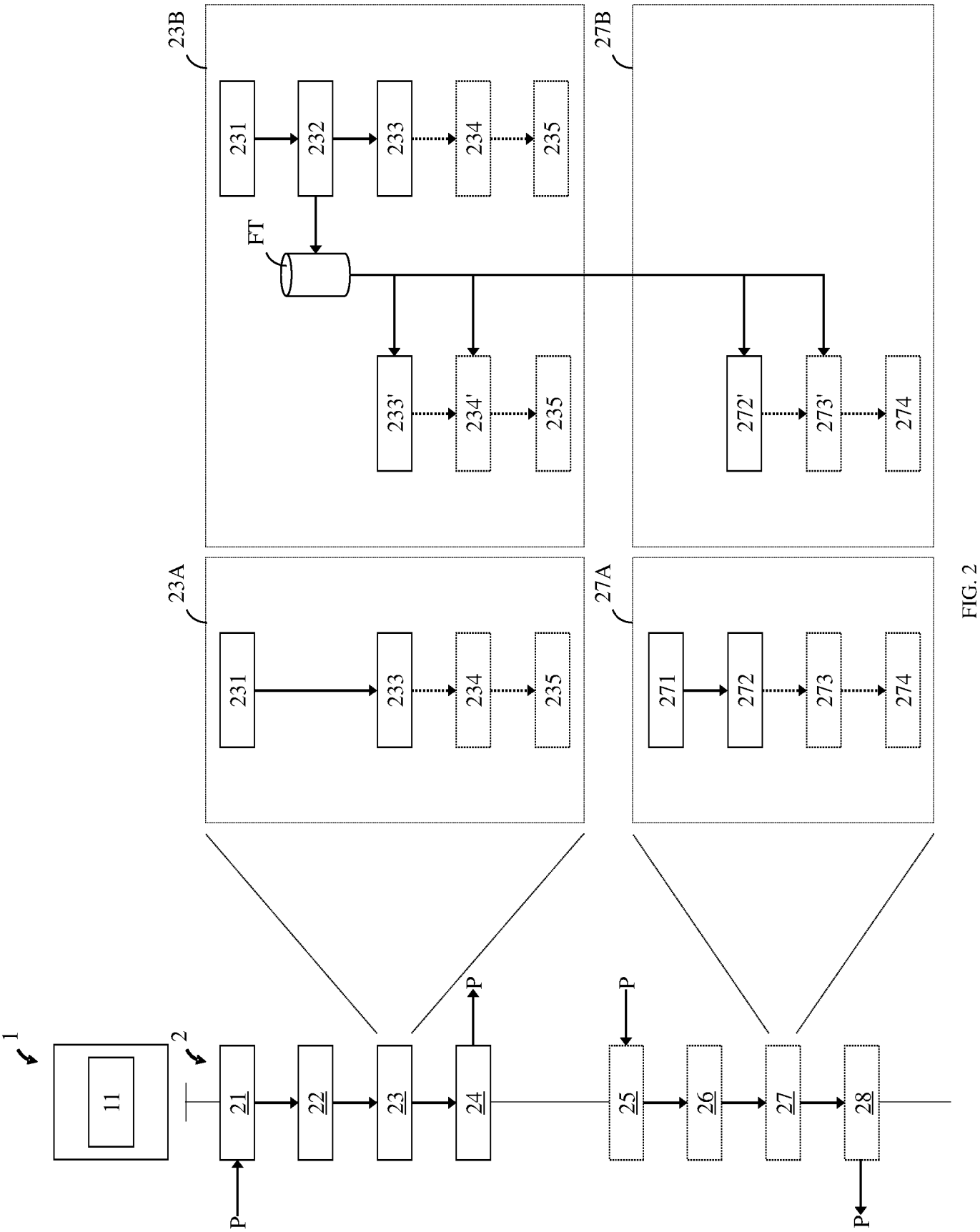
1
11
2
21
22
23
24
25
26
27
28
P
P
P
23A
231
233
234
235
23B
231
232
233
234
235
FT
233'
234'
235
27A
271
272
273
274
27B
272'
273'
274

FIG. 2

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2021/083527

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L9/00 H04L9/40 H04L61/2539
ADD. H04L101/668

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L

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

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal, WPI Data, COMPENDEX, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 9 641 434 B1 (LAURENCE DOUGLAS STEWART [US] ET AL) 2 May 2017 (2017-05-02) column 2, line 52 - column 13, line 46 -----	1-25
X	US 6 826 684 B1 (FINK RUSSELL ANDREW [US] ET AL) 30 November 2004 (2004-11-30) column 5, line 51 - column 17, line 37 ----- -/--	1-25

[x] Further documents are listed in the continuation of Box C.

[x] See patent family annex.

* Special categories of cited documents :

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

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

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
6 July 2022	15/07/2022

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Böhmert, Jörg

1

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2021/083527

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	KEWLEY D ET AL: "Dynamic approaches to thwart adversary intelligence gathering", DARPA INFORMATION SURVIVABILITY CONFERENCE & EXPOSITION II, 2001. DISC EX '01. PROCEEDINGS 12-14 JUNE 2001, PISCATAWAY, NJ, USA,IEEE, vol. 1, 12 June 2001 (2001-06-12), pages 176-185, XP010549121, ISBN: 978-0-7695-1212-9 Section 3 on pages 177ff; figure 3 -----	1-25
A	US 7 916 739 B2 (NTT DOCOMO INC [JP]) 29 March 2011 (2011-03-29) column 3, line 10 - column 11, line 50 -----	1-25

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2021/083527

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 9641434 B1	02-05-2017	NONE	
US 6826684 B1	30-11-2004	NONE	
US 7916739 B2	29-03-2011	JP 4464963 B2	19-05-2010
		JP 2007521749 A	02-08-2007
		US 2005041675 A1	24-02-2005
		WO 2005006663 A1	20-01-2005