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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
26 June 2014 (26.06.2014)

WIPO | PCT

(10) International Publication Number
WO 2014/098562 A2

(51) International Patent Classification:
H04L 29/06 (2006.01)

(21) International Application Number:
PCT/MY2013/000259

(22) International Filing Date:
18 December 2013 (18.12.2013)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
PI 2012005529 20 December 2012 (20.12.2012) MY

(71) Applicant: **MIMOS BERHAD** [MY/MY]; Technology Park Malaysia, Kuala Lumpur, 57000 (MY).

(72) Inventors: **ABDULLAH, Mohd Ariff**; Mimos Berhad, Technology Park Malaysia, Kuala Lumpur, 57000 (MY). **HASEEB, Shariq**; Mimos Berhad, Technology Park Malaysia, Kuala Lumpur, 57000 (MY). **MOHD EZANI, Muhammad Faheem**; Mimos Berhad, Technology Park Malaysia, Kuala Lumpur, 57000 (MY).

(74) Agent: **NANJAPPAN, Puvaneswari**; Kass International Sdn. Bhd., Suite 8-7-2, Menara Mutiara Bangsar, Jalan Liku, Off Jalan Riong, Kuala Lumpur, 59100 (MY).

(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, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, 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, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(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, 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,

[Continued on next page]

(54) Title: A SYSTEM AND A METHOD FOR FACILITATING MOBILE INTERNET PROTOCOL COMMUNICATION

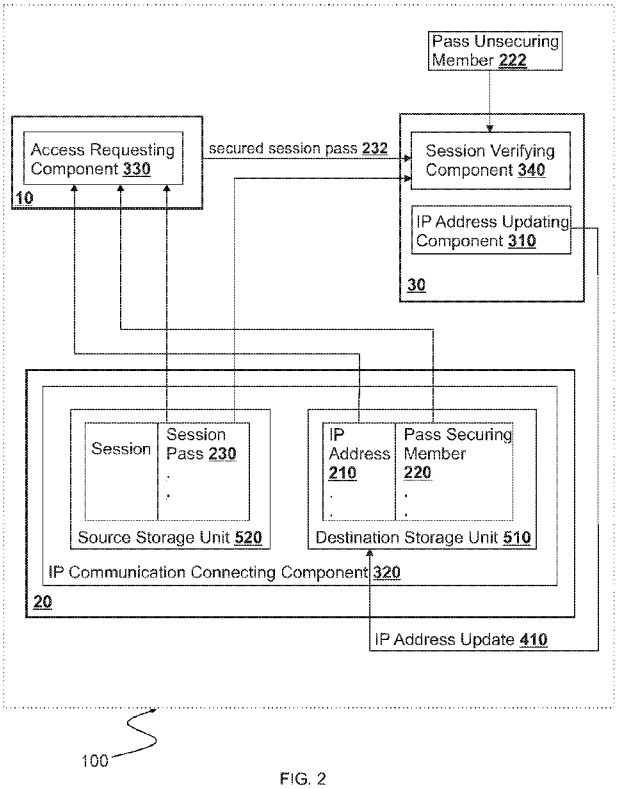

FIG. 2

(57) Abstract: The present invention relates to a system (100) and a method for facilitating mobile Internet Protocol (IP) communication. The system (100) comprises an IP address updating component (310) residing in a mobile destination terminal (30), an IP communication connecting component (320) residing in a transit terminal (20), an access requesting component (330) residing in a source terminal (10), and a session verifying component (340) residing in the mobile destination terminal. The system (100) and the method revolves around keeping track of the mobile destination terminal (30), keeping track of the communication session between the mobile destination terminal (30) and the source terminal (10). The system (100) and the method revolve around the authentication and mobility purposes. FIG. 2

WO 2014/098562 A2

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:

— *without international search report and to be republished upon receipt of that report (Rule 48.2(g))*

A SYSTEM AND A METHOD FOR FACILITATING MOBILE INTERNET PROTOCOL COMMUNICATION

FIELD OF THE INVENTION

The present invention relates to a system and a method for facilitating mobile Internet Protocol (IP) communication.

BACKGROUND ART

It is true that it is impossible for data to travel as it is in its original format. When the data are required to travel through a connected network for example through the Internet or through a more cumbersome platform i.e. the mobile IP communication network, the data is required to travel in packets. In other words, it is required to be encapsulated in packets first.

Further to the above, the reason behind encapsulating the data in packets is to facilitate the data to be interpretable by an end recipient, and at the same time to ensure that the data is properly addressed to the recipient. As a comparison, those data is just like in real life in which messages are written on a letter to be sent out as mails to the correct recipient. In this connection, every network terminal, for instance a source terminal, a destination terminal and even a transit terminal contain their own IP address to signify their location with respect to the network area they are in.

As such, it is common to observe that these data packets contain a body where the data is contained and a number of headers that serve to indicate the address of the recipient such that the packets can be sent to the right recipient.

Another important factor to ponder is the security of these packets. As the packets are required to travel through unsecured channels for example through what has been considered as vulnerable IP network for example through the Internet or through the mobile IP communication network.

As discussed above, the data being encapsulated in the packets achieve three main objectives i.e. the capacity to carry a load i.e. the data through an IP network, to bridge the inconsistency between transmission protocol between or among the diverse networks,

and to safeguard the privacy of those data that are usually sensitive and vulnerable to being breached.

In view of the above, it seems that the existing technology i.e. the existing IP tunneling is, prima facie, able to address such problems and achieve such objectives. Particularly to deliver the packets from a source terminal i.e. a corresponding node to a mobile destination terminal i.e. a mobile node, the utilization of the mobile IP tunneling is common.

In a mobile network environment, there exist differences in terms of routing protocols between the networks systems i.e. between the source network and the mobile destination network. As such, it is imperative to bridge the differences in terms of the routing protocols between the network systems. Thus, the mobile IP tunneling has been introduced.

The mobile IP tunneling generally revolves around forwarding the packets first to a redirecting server (usually called a home agent) and encapsulating the packets with headers (to incorporate the IP address for the intended recipient) before forwarding those packets to the rightful IP recipients. In other words, the mobile IP tunneling is a protocol in a mobile IP environment that involves using encapsulating payload protocol through a delivery protocol. The payload protocol has been defined as the IP communication between a mobile destination terminal and a source terminal whereas the delivery protocol is the IP communication between the mobile destination terminal and a transit terminal.

As mentioned above, due to the security concerns, these packets are also required to be encrypted. Besides the packets' encryption, their headers are generally encrypted as well. The headers are encrypted such that no other outsiders or non-intended reader can detect the initial source sender's IP address as well as the intended recipient's address. Such an encryption of the headers entails another level of encapsulation of the packets i.e. the previously encapsulated packets have to be encapsulated again in yet another layer of encapsulation as illustrated in FIG. 1.

The tunneled packet only traverses and lasts for only a certain displacement as ultimately, the packets would be de-encapsulated such that the packet would travel to its intended location on itself. At the outset, this may seem a bit inconvenient because it involves encapsulation and de-encapsulation process which do seem quite undesirable.

However, upon closer inspection and multiple usages in our daily life, this mobile IP tunneling could bring other sorts of shortcomings. With reference to FIG. 1, during transmission from a transit terminal to a mobile destination terminal, additional data capacity for example bits are required in the payload (the body containing the data) in order to accommodate the increasing tunneled header with respect to the pre-tunneled header. As a consequence, the tunneled payload decreases as compared to the pre-tunneled payload.

Looking closer to the FIG. 1, the load (space) for the headers seems to have expanded in light of that the stacked (nested tunnels) nature of the packets and thus, there no longer left enough room for the payload data itself. As such, there are less data per an IP packet. Moreover, this results to lower throughput in terms of payload.

The situation would be more dire if the size of the tunneled packets carrying many layers of stacked headers (as seen in FIG. 1) surpass the size limit for example the Maximum Transmission Unit (MTU). The packet could be fragmentized resulting to overhead and latency issues.

Among other things, the transit terminal which serves to receive and redirect the packets to the mobile destination terminal is deemed quite cumbersome. Other than that, it does seem that the transit of packeted data through a transit terminal “lengthen” the distance between the mobile destination terminal and the source terminal.
In light of the above, a system and a method for facilitating mobile IP communication that overcome above shortcomings is very much in need.

SUMMARY OF THE INVENTION

According to the present invention, there is provided a system (100) and a method for facilitating mobile Internet Protocol (IP) communication.

According to one aspect of the present invention, the system comprises an IP address updating component residing in a mobile destination terminal, an IP communication connecting component residing in a transit terminal, an access requesting component residing in a source terminal, and a session verifying component residing in an intended mobile destination terminal. The IP communication connecting component comprises a destination storage unit and a source storage unit. The session verifying component comprises a pass unsecuring number.

The IP address updating component identifies a current IP address of the mobile destination terminal, and forwards an IP address update to the IP communication connecting component. The IP communication connecting component receives and stores the current IP address of the mobile destination terminal on the destination storage unit. The destination storage unit is adapted for storing data related to the mobile destination terminal. The data comprises the IP addresses of the mobile destination terminal and a pass securing member of the mobile destination terminal.

The access requesting component forwards a request to establish an IP connection with an intended mobile destination terminal. The IP communication connecting component receives and stores the request in the source storage unit, generates a session pass upon receipt of the request, and forwards the session pass to the session verifying component of the intended mobile destination terminal, and retrieves the IP address and the pass securing member from the destination storage unit, and forwards the IP address, the pass securing member, and the session pass to the access requesting component of the source terminal.

The access requesting component secures the session pass with the pass securing member, and forwards the secured session pass to the IP address of the intended mobile destination terminal. The session verifying component unsecures the secured session pass with the pass unsecuring member of the session verifying component, compares the unsecured session pass with the session pass received from the IP communication connecting component, determines whether both of the session passes match with each other, and establishes the IP connection with the source terminal if both of the session passes match.

In accordance with another aspect of the present invention, there is provided a transit terminal, wherein the transit terminal comprises an IP communication connecting component, the IP communication connecting component generates a new session pass on receipt of a access request received from a source terminal to establish an IP connection with an intended mobile destination terminal, the IP communication connecting component further forwards the session pass to the source terminal and the intended mobile destination terminal associated with the access request.

According to yet another aspect of the present invention, the method comprising the steps of identifying a current IP address of a mobile destination terminal and forwarding an IP address update to an IP communication connecting component of the system using an IP

address updating component of the system; receiving and storing the current IP address of the mobile destination terminal on a destination storage unit using the IP communication connecting component, the destination storage unit being for storing data related to the mobile destination terminal; forwarding a request to establish an IP connection with an intended mobile destination terminal using an access requesting component; receiving and storing the request in the source storage unit using the IP communication connecting component; generating a session pass upon receipt of the request using the IP communication connecting component; forwarding the session pass to a session verifying component of the intended mobile destination terminal using the IP communication connecting component; retrieving the IP address and a pass securing member from the destination storage unit, and forwarding the IP address, the pass securing member, and the session pass to the access requesting component of the source terminal using the IP communication connecting component; securing the session pass with the pass securing member, and forwarding the secured session pass to the IP address of the intended mobile destination terminal using the access requesting component; and unsecuring the secured session pass with a pass unsecuring member, comparing the unsecured session pass with the session pass received from the IP communication connecting component, determining whether both of the session passes match with each other, and establishing the IP connection with the source terminal if both of the session passes match using a session verifying component. The session verifying component resides in the mobile destination terminal; and the session verifying component having a pass unsecuring member.

The IP address updating component resides in the mobile destination terminal whereas the IP communication connecting component resides in a transit terminal.

The IP communication connecting component comprises a destination storage unit and a source storage unit. The data comprises the IP addresses of the mobile destination terminal and the pass securing member in relation to the mobile destination terminal;
It is an object of the present invention to provide a system and a method for facilitating mobile IP communication without the mobile IP tunneling.

It is also an object of the present invention to provide a system and a method for facilitating mobile IP communication that reduces the data capacity (i.e. the quantity space of the data) required in a header of a carrier packet for carrying the payload from the source terminal to the mobile destination terminal, therefore increasing the data capacity of a body of the carrier packet itself for example with respect to mobile IP tunneling. In

short, the delivery of more data in one IP packet is expected that also signifies a higher throughput of data for example in comparison to the mobile IP tunneling.

It is also an object of the present invention to provide a system and a method for facilitating mobile IP communication that can do away without encapsulation of data packets like in the IP tunneling in order to provide a smoother delivery of data. No de-encapsulating of the data packets is required too.

It is further an object of the present invention to provide a system and a method for facilitating IP communication that can do away without through a transit terminal i.e. an on-behalf receiving server like a redirecting server.

It is also an object of the present invention to provide a system and a method for facilitating IP communication that shorten the path for the traveling IP packets between a source terminal and a mobile destination terminal.

It is also an object of the present invention to provide a system and a method for facilitating mobile IP communication that prevent the size of the carrier packet from exceeding the possible size limit of the carrier packet itself, for example exceeding the Maximum Transmission unit (MTU) such that the packet would not be fragmentized and that problems like overhead and latency can be avoided.

It is further object of the present invention to provide a system and a method for facilitating mobile IP communication that track the mobility of the mobile destination terminal for example in the absence of the mobile IP tunneling.

It is further object of the present invention to provide a system and a method for facilitating mobile IP communication that track the communication sessions between the mobile destination terminal and the source terminal for example in the absence of the mobile IP tunneling.

It is also an object of the present invention to provide a system and a method for facilitating mobile IP communication that can recognize the identity of a mobile destination terminal that move between or among networks for example in the absence of the mobile IP tunneling.

It is also an object of the present invention to provide a system and a method for facilitating mobile IP communication that assist a mobile destination terminal to verify a source terminal in a mobile IP communication for example in the absence of the mobile IP tunneling.

It is also final object of the present invention to provide a system and a method for facilitating mobile IP communication in which a session pass can be provided from the transit terminal to the source terminal and the mobile destination terminal such that the session can be secured by the access requesting component of the source terminal using a pass securing member and can be unsecured by the session verifying component of the mobile destination terminal using a pass unsecuring member such that the security of the mobile IP communication can be maintained in a mobile environment for example in the absence of the mobile IP tunneling.

The present invention consists of certain novel features and a combination of parts hereinafter fully described and illustrated in the accompanying drawings and particularly pointed out in the appended claims; it being understood that various changes in the details may be without departing from the scope of the invention or sacrificing any of the advantages of the present invention.

BRIEF DESCRIPTION OF THE DRAWINGS

For the purpose of facilitating an understanding of the invention, there is illustrated in the accompanying drawings the preferred embodiments from an inspection of which when considered in connection with the following description, the invention, its construction and operation and many of its advantages would be readily understood and appreciated.

FIG. 1 shows the Internet Protocol (IP) flow of the data packet between networks from a source terminal to a mobile destination terminal using the conventional mobile IP tunneling.

FIG. 2 shows a diagram depicting the linkage of all the components involved in the system and the method of the present invention.

FIG. 3 shows a flowchart depicting the top level flow involved in the method of the present invention.

FIG. 4 shows a flowchart depicting the IP address update in an IP address updating component of a mobile destination terminal of the present invention.

FIG. 5 shows a flowchart depicting the IP address update in an IP communication connecting component of a transit terminal of the present invention.

FIG. 6 shows a flowchart depicting the session assignment in the IP communication connecting component of the transit terminal of the present invention.

FIG. 7 shows a flowchart depicting the session assignment in the access requesting component of a source terminal of the present invention.

FIG. 8 shows a flowchart depicting another example of a session assignment in the access requesting component of a source terminal of the present invention.

FIG. 9 shows a flowchart depicting the session assignment in a session verifying component of the mobile destination terminal of the present invention.

FIG. 10 shows how the IP address updating component of the mobile destination terminal updates the IP communication connecting component of the transit terminal.

FIG. 11 shows how the access requesting component of the source terminal requests the IP communication connecting component for an IP session.

FIG. 12 shows how the IP communication connecting component forwards the session pass to the access requesting component, and the session pass, the IP address, and the pass securing member to the session verifying component.

FIG. 13 shows how the access requesting component forwards the session pass secured using the pass securing member to the session verifying component.

FIG. 14 shows how the session verifying component unsecures the received secured session pass to verify the source terminal and once the IP connection between the source terminal and the mobile destination terminal is established, the mobile destination terminal starts to receive data packets from the source terminal.

FIG. 15 shows how the IP address updating component updates the IP communication connecting component when the mobile destination terminal changes its position therefore changing its IP address (receiving from other most adjacent local network), whilst the IP communication connecting component updates the destination storage unit.

FIG. 16 shows that when the source terminal reaches a timeout, the access requesting component forwards a request to establish an IP connection using the existing session pass.

FIG. 17 shows how the IP communication connecting component assigns a new session pass.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

The present invention relates to a system (100) and a method for facilitating mobile IP communication. Hereinafter, the system (100) and the method shall be described according to the preferred embodiments of the present invention and by referring to the accompanying description and drawings. However, it is to be understood that limiting the description to the preferred embodiments of the invention and to the drawings is merely to facilitate discussion of the present invention and it is envisioned that those skilled in the art may devise various modifications without departing from the scope of the appended claim.

Referring to FIG. 2, according to one aspect of the present invention, the system (100) for facilitating mobile Internet Protocol (IP) communication is shown. The system (100) comprises an IP address updating component (310), an IP communication connecting component (320), an access requesting component (330), and a session verifying component (340).

Referring to FIG. 1 & 2, the IP address updating component (310) and the session verifying terminal (340) reside in a mobile destination terminal (30). The IP communication connecting component (320) resides in a transit terminal (20). The access requesting component (330) resides in a source terminal (10).

Referring to FIG. 2 again, the IP communication connecting component (320) comprises a destination storage unit (510) and a source storage unit (520). The session verifying component (340) comprises a pass unsecuring member (222).

Ultimately, the IP communication connecting component (320) tracks the IP address (210) of the mobile destination terminal (30) through the destination storage unit (510), and handles the IP connection between the source terminal (10) and the mobile destination terminal (30) through the source storage unit (520).

Referring to FIG. 2, 4, & 10, the IP address updating component (310) identifies the current IP address (210) of the mobile destination terminal (30). The IP address updating component (310) achieves this by detecting whether there is any change in the network attached to the mobile destination component (30). If this is the case, this indicates that there is a change in the current IP address (210) of the mobile destination terminal (30) and the IP address updating component (310) only forwards an IP address update (410) to the IP communication connecting component (320). Ultimately, the IP address updating component (310) is adapted to update the IP communication connecting component (320) regarding the current IP address (210) of the mobile destination terminal (30). An example regarding the change of network attached to the mobile destination network (30) is also illustrated in FIG. 15-17.

Referring now to FIG. 2 & 5, the IP communication connecting component (320) receives and stores the current IP address (210) of the mobile destination terminal (30) on the destination storage unit (510). The destination storage unit (510) is adapted to store data related to the mobile destination terminal (30). The data comprise the IP addresses (210) of the mobile destination terminal (30) and a pass securing member (220) in relation to the mobile destination terminal (30).

As shown in FIG. 5, the IP communication connecting component (320), upon receiving the current IP address (210) of the mobile destination terminal (30) from the IP update address updating component (310), checks whether the current IP address (210) has already been stored in the destination storage unit (510); if the current IP address (210) has been stored in the destination storage unit (510); the destination storage unit (510) is updated; and if the current IP address (210) has not been stored in the destination storage unit (510); and the current IP address (210) is stored as a new IP address (210) in the destination storage unit (510).

With reference to FIG. 2 & 11, the access requesting component (330) forwards a request to establish an IP connection with an intended mobile destination terminal (32). As shown in FIG. 2, 6 & 12, the IP communication connecting component (320) is adapted further for, not in any particular order, receiving and storing the request in the source storage unit

(520), generating and assign a session pass (230) upon receipt of the request; forwarding the session pass (230) to the session verifying component (340) of the intended mobile destination terminal (32), and retrieving the IP address (210) and the pass securing member (220) from the destination storage unit (510), and forwarding the IP address (210), the pass securing member (220), and the session pass (230) to the access requesting component (330). The above mentioned order is allowed to follow that shown in FIG. 6.

Referring to now to FIG. 2, 7, 8, & 13, the access requesting component (330) further secures the session pass (230) with the pass securing member (220), and forwards the secured session pass (232) to the IP address (210) of the intended mobile destination terminal (32).

Referring to FIG. 7, if the source terminal (10) reaches a timeout, the access requesting component (330) forwards a new request to establish an IP connection with the intended mobile destination terminal (32) using the previously received session pass (230), the IP communication connecting component (320) receives and stores the request in the source storage unit (520), generates a new session pass (230) upon receipt of the request, and forwards the new session pass (230) to the intended mobile destination terminal (32) and the source terminal (10). If the access requesting component (330) has not received the IP address (210), the pass securing member (220), and the session pass (230) from the IP communication connecting component (320), and if the timeout has not been reached, the access requesting component (330) waits for the receipt of the IP address (210), the pass securing member (220), and the session pass (230) from the IP communication connecting component (320). FIG. 8 shows slightly a difference route with regards the error before receiving a reply from the IP communication connecting component (320).

FIG. 9 shows the route of steps involved in the session verifying component (340). The session verifying component (340) unsecures the secured session pass (232) with the pass unsecuring member (222), compares the unsecured session pass (232) with the session pass (230) received from the IP communication connecting component (320), determines whether both of the session passes (230) match with each other, and establishes the IP connection with the source terminal (10) if both of the session passes (230) match as shown in FIG. 9 & 14.

As an example, the source terminal (10) is a corresponding node, the transit terminal (20) is a redirect server, the mobile destination terminal (30) and the intended mobile

destination terminal (32) each are a mobile node. The destination storage unit (510) comprises a binding table (510). The source storage unit (520) comprises a correspondent table (520). The pass securing member (220) is a public key (220) whereas the pass unsecuring member (222) is a private key.

Referring to FIG. 2, & 10-17, the binding table (510) is adapted for keeping track of the mobile node. The correspondent table (520) is adapted for keeping track of the communication sessions between the mobile nodes and the corresponding nodes. The public key (220) is used in a public key distribution for an authentication purpose, whereas the session key (230) is used in a session key (230) distribution for a mobility purpose.

Referring to FIG. 2-17, according to another aspect of the present invention, the method for facilitating mobile Internet Protocol (IP) communication is implemented using the system (100). The method comprises the steps of

identifying a current IP address of a mobile destination terminal and forwarding an IP address update to an IP communication connecting component of the system using an IP address updating component of the system; receiving and storing the current IP address of the mobile destination terminal on a destination storage unit using the IP communication connecting component, the destination storage unit being for storing data related to the mobile destination terminal; forwarding a request to establish an IP connection with an intended mobile destination terminal using an access requesting component; receiving and storing the request in the source storage unit using the IP communication connecting component; generating a session pass upon receipt of the request using the IP communication connecting component; forwarding the session pass to a session verifying component of the intended mobile destination terminal using the IP communication connecting component; retrieving the IP address and a pass securing member from the destination storage unit, and forwarding the IP address, the pass securing member, and the session pass to the access requesting component of the source terminal using the IP communication connecting component; securing the session pass with the pass securing member, and forwarding the secured session pass to the IP address of the intended mobile destination terminal using the access requesting component; and unsecuring the secured session pass with a pass unsecuring member, comparing the unsecured session pass with the session pass received from the IP communication connecting component, determining whether both of the session passes match with each other, and establishing the IP connection with the source terminal if both of the session passes match using a session verifying component. The session verifying

component resides in the mobile destination terminal; and the session verifying component having a pass unsecuring member.

Referring now to FIG. 1 & 2, the IP address updating component (310) and the session verifying terminal (340) reside in a mobile destination terminal (30). The IP communication connecting component (320) resides in a transit terminal (20). The access requesting component (330) resides in a source terminal (10).

Referring to FIG. 2 again, the IP communication connecting component (320) comprises the destination storage unit (510) and the source storage unit (520). The session verifying component (340) comprises the pass unsecuring member (222).

The system (100) comprises an IP address updating component (310), an IP communication connecting component (320), an access requesting component (330), and a session verifying component (340).

Ultimately, the IP communication connecting component (320) tracks the IP address (210) of the mobile destination terminal (30) through the destination storage unit (510), and handles the IP connection between the source terminal (10) and the mobile destination terminal (30) through the source storage unit (520).

Referring to FIG. 2, 4, & 10, the step of forwarding an IP address update (410) to an IP communication connecting component (320) further comprises the step of forwarding the IP address update (410) to the IP communication connecting component (320) when there is a change in the current IP address (210) of the mobile destination terminal (30). An example regarding the change of network attached to the mobile destination terminal (30) is illustrated in FIG. 15-17.

With reference to FIG. 2 & 5, the step of receiving and storing the current IP address (210) of the mobile destination terminal (30) on the destination storage unit (510) further comprises the steps of checking whether the current IP address (210) has been stored in the destination storage unit (510), and updating the destination storage unit (510); wherein if the current IP address (210) has been stored in the destination storage unit (510), the destination storage unit (510) is updated; and if the current IP address (210) has not been stored in the destination storage unit (510), the current IP address (210) is stored as a new IP address (210) in the destination storage unit (510).

Referring to FIG. 7, the method further comprises the steps of:

if the source terminal (10) reaches a timeout, forwarding a new request to establish an IP connection with the intended mobile destination terminal (32) with the previously received session pass (230) using the access requesting component (330);

receiving and storing the request in the source storage unit (520), generating a new session pass (230) upon the request, and forwarding the new session pass (230) to the intended mobile destination terminal (32) and the source terminal (10) using the IP communication connecting component (320);

if the access requesting component (330) has not received the IP address (210), the pass securing member (220), and the session pass (230) from the IP communication connecting component (320), and if the timeout has not been reached, waiting for the receipt of the IP address (210), the pass securing member (220), and the session pass (230) from the IP communication connecting component (320) using the access requesting component (330).

For example, the source terminal (10) is a corresponding node, the transit terminal (20) is a redirect server, the mobile destination terminal (30) and the intended mobile destination terminal (32) each are a mobile node. The destination storage unit (510) comprises a binding table (510) whereas the source storage unit (520) comprises a correspondent table (520). The pass securing member (220) is a public key (220) whereas the pass unsecuring member (222) is a private key.

Referring to FIG. 2, & 10-17, the binding table (510) is adapted to keep track of the mobile node. The correspondent table (520) is adapted to keep track of the communication sessions between the mobile nodes and the corresponding nodes. The public key (220) is used in a public key distribution for an authentication purpose, whereas the session key (230) is used in a session key (230) distribution for a mobility purpose.

While in the foregoing specification this invention has been described in relation to certain preferred embodiments thereof and many details have been set forth for purpose of illustration, it will be apparent to those skilled in the art that the invention is susceptible to additional embodiments and that certain of the details described herein can be varied considerably without departing from the basic principles of the invention.

CLAIMS

1. A system (100) for facilitating mobile Internet Protocol (IP) communication comprising:

(i) at least one source terminal (10), wherein said source terminal (10) comprises an access requesting component (330), wherein said access requesting component (330) is adapted to raise an access request and to generate a secured session pass (232) to establish an IP connection with an intended mobile destination terminal (32);

(ii) at least one transit terminal (20) comprising an IP communication connecting component (320), said IP communication connecting component (320) is adapted to generate a new session pass (230) on receipt of said access request received from a source terminal (10), said IP communication connecting component (320) is further adapted to forward said session pass (230) to a source terminal (10) and an intended mobile destination terminal (32) associated with said access request; and

(iii) at least one mobile destination terminal (30), wherein said mobile destination terminals (30) being associated with discrete dynamic IP address (210), a pass securing member (220) and a pass unsecuring member (222), wherein said mobile destination terminal (30) having a session verifying component (340), said session verifying component (340) is adapted to unsecure a secured session pass (232) received from a source terminal (10) using said pass unsecuring member (222), compare a unsecured session pass (232) with said session pass (230) received from said transit terminal (20) and establish an IP communication session with a corresponding source terminal (10) if both the session pass match.

2. The system as claimed in claim 1, wherein said IP communication connecting component (320) is further adapted to receive and store a current IP address (210) and a pass securing member (220) associated with said mobile destination terminal (30), said IP communication connecting component (320) having:

(i) a destination storage unit (510) for storing data including said current IP address (210) and said pass securing member (220) in relation to said mobile destination terminal (30); and

(ii) and a source storage unit (520) to store said access requests raised by said source terminal (10);

wherein said IP communication connecting component (320) tracks the IP address (210) of said mobile destination terminal (30) through said destination storage unit (510), and handles the IP connection between said source terminal (10) and said mobile destination terminal (30) through said source storage unit (520); and said IP communication connecting component (320) further upon receiving a current IP address (210) of said mobile destination terminal (30) checks whether the current IP address (210) has already been stored in the destination storage unit (510) and updates said destination storage unit (510) with the current IP address (210) as the new IP address (210) if the current IP address (210) has not been stored in the destination storage unit (510).

3. The system (100) as claimed in claim 1, wherein and said source terminal (10) associated with said access request is further adapted to receive a session pass (230), a current IP address (210) and a pass securing member associated with an intended mobile destination terminal (32) from said transit terminal (20) to generate said secured session pass (232) using said access requesting component (330).

4. The system (100) as claimed in claim 1, wherein said access requesting component (330) is further adapted to forward a new access request using the previously received session pass (230) if said source terminal (20) reaches a timeout while waiting for said session pass (230) from said transit terminal (20); said IP communication connecting component (320) receives and stores the request, generates a new session pass (230) upon receipt of the request, and forwards the new session pass (230) to said intended mobile destination terminal (32) and said source terminal (10); and if said access requesting component (330) has not received the IP address (210), said pass securing member (220), and said session pass (230) from the IP communication connecting component (320), and if the timeout has not been reached, the access requesting component (330) waits for the receipt of the IP address (210), the pass securing member (220), and the session pass (230) from the IP communication connecting component (320).

5. The system (100) as claimed in claim 1, wherein said mobile destination terminal (30) further includes an IP address updating component (310) adapted to identify and forward a current IP address (210) of said mobile destination terminal (30) to said IP communication connecting component (320) when there is a change in the current IP address (210) of said mobile destination terminal (30).

6. A transit terminal (20) for use in the system (100) as described in claim 1, wherein said transit terminal (20) comprises an IP communication connecting component (320), said IP communication connecting component (320) is adapted to generate a new session pass (230) on receipt of a access request received from a source terminal (10) to establish an IP connection with an intended mobile destination terminal (32), said IP communication connecting component (320) is further adapted to forward said session pass (230) to said source terminal (10) and said intended mobile destination terminal (32) associated with said access request.

7. A method for facilitating mobile Internet Protocol (IP) communication, the method is implemented using a system (100) for facilitating the mobile IP communication, the method comprising the following steps:

(i) identifying a current IP address (210) of a mobile destination terminal (30) and forwarding an IP address update (410) to an IP communication connecting component (320) using an IP address updating component (310), wherein said IP communication connecting component (320) resides in a transit terminal (20) and said IP address updating component (310) resides in said mobile destination terminal (30) and said mobile destination terminal (30) being associated with a discrete pass securing member (220) and a pass unsecuring member (222);

(ii) facilitating a source terminal to raise an access request to establish an IP connection with an intended mobile destination terminal (32) using an access requesting component (330), wherein said access requesting component residing in a source terminal (10);

(iii) generating a new session pass (230) at said transit terminal corresponding to said access request using said IP communication connecting component (320);

(iv) forwarding said session pass (230) to a session verifying component (340) residing in said intended mobile destination terminal (32) and said access requesting component (330) using the IP communication connecting component (320);

(v) securing the session pass (230) with the pass securing member (220), and forwarding the secured session pass (232) to the current IP address (210) of the intended mobile destination terminal (32) using the access requesting component (330); and

(vi) unsecuring the secured session pass (232) with said pass unsecuring member (222), comparing the unsecured session pass (232) with the session pass (230) received from the IP communication connecting component (320), and

establishing the IP connection with the source terminal (10) if both of the session passes (230) match using said session verifying component (340).

8. The method as claimed in claim 7, wherein the step of identifying a current IP address (210) of a mobile destination terminal (30) includes the steps of checking whether the current IP address (210) has been stored on a destination storage unit (510) hosted in IP communication connecting component (320) and updating the destination storage unit (510) along with said pass securing member (220) in relation to said mobile destination terminal (30); wherein if the current IP address (210) has been stored in said destination storage unit (510), said destination storage unit (510) is updated; and if said current IP address (210) has not been stored in said destination storage unit (510), said current IP address (210) is stored as a new IP address (210) in said destination storage unit (510).

9. The method as claimed in claim 7, wherein the step of facilitating a source terminal to raise an access request to establish an IP connection with an intended mobile destination terminal (32) comprises the following steps:

(i) determining if the source terminal (10) reaches a timeout while waiting for said session pass (230) from said transit terminal (20), forwarding a new request to establish an IP connection with the intended mobile destination terminal (32) with the previously received session pass (230) using the access requesting component (330) in the event of said timeout;

(ii) receiving and storing the request in the source storage unit (520), generating a new session pass (230) upon the request, and forwarding the new session pass (230) to the intended mobile destination terminal (32) and the source terminal (10) using the IP communication connecting component (320); and

(iii) verifying if the access requesting component (330) has not received the IP address (210), the pass securing member (220), and the session pass (230) from the IP communication connecting component (320), and if the timeout has not been reached, waiting for the receipt of the IP address (210), the pass securing member (220), and the session pass (230) from the IP communication connecting component (320) using the access requesting component (330).

10. The method as claimed in claim 7, wherein the step of generating a new session pass (230) at a transit terminal includes the following steps:

(i) storing the access request in said IP communication connecting component (320); and

(ii) retrieving the IP address (210) and said pass securing member (220) from said IP communication connecting component (320), and forwarding the IP address (210), the pass securing member (220), and the session pass (230) to the access requesting component (330) of said source terminal (10) using said IP communication connecting component (320).

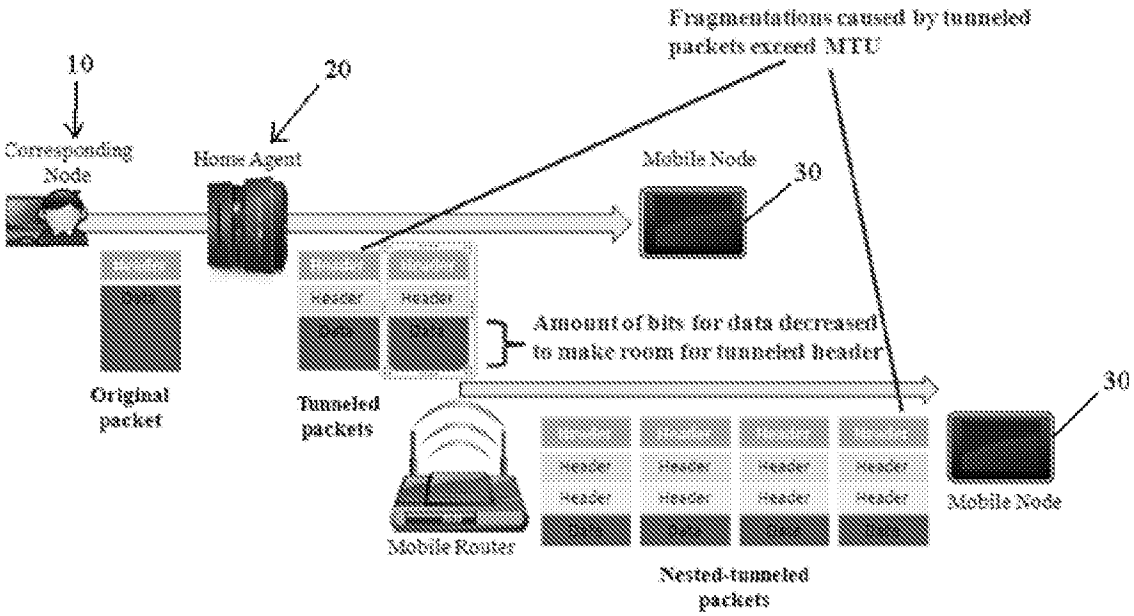
Fragmentations caused by tunneled packets exceed MTU
10
20
Corresponding Node
Home Agent
Mobile Node
30
Header
Amount of bits for data decreased to make room for tunneled header
Original packet
Tunneled packets
Mobile Router
Nested-tunneled packets
30
Mobile Node

FIG. 1

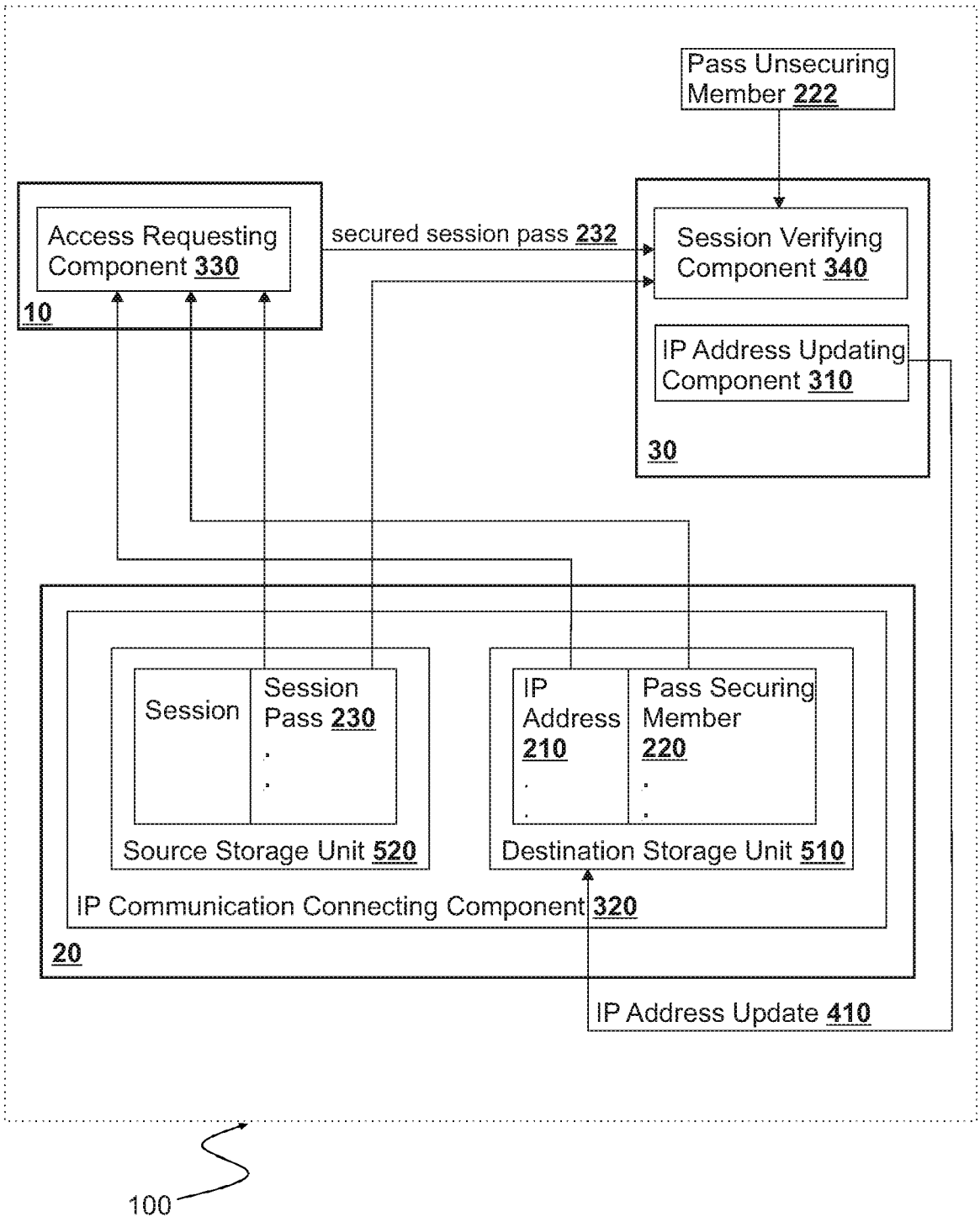
Pass Unsecuring Member 222
Access Requesting Component 330
10
secured session pass 232
Session Verifying Component 340
IP Address Updating Component 310
30
Session
Session Pass 230
Source Storage Unit 520
IP Address 210
Pass Securing Member 220
Destination Storage Unit 510
IP Communication Connecting Component 320
20
IP Address Update 410
100

FIG. 2

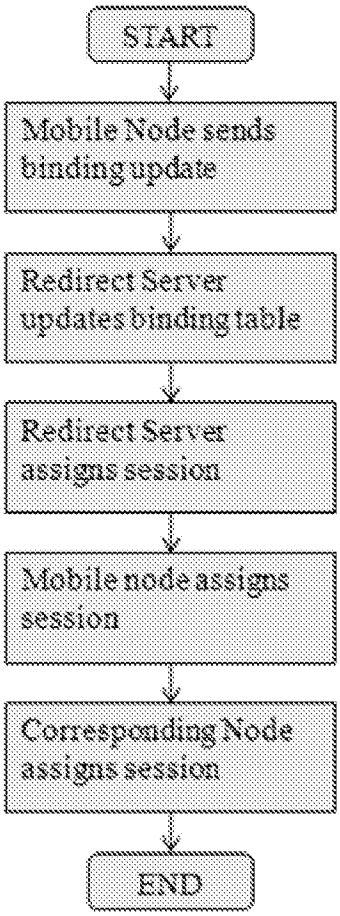
START
Mobile Node sends binding update
Redirect Server updates binding table
Redirect Server assigns session
Mobile node assigns session
Corresponding Node assigns session
END

FIG. 3

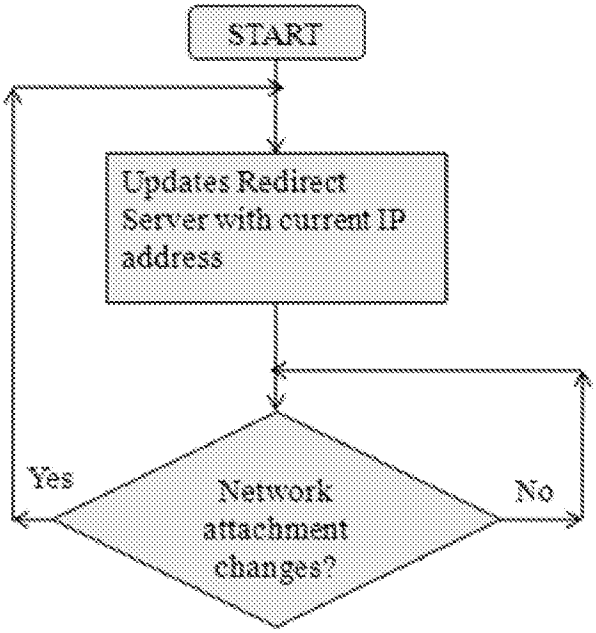
START
Updates Redirect Server with current IP address
Network attachment changes?
Yes
No

FIG. 4

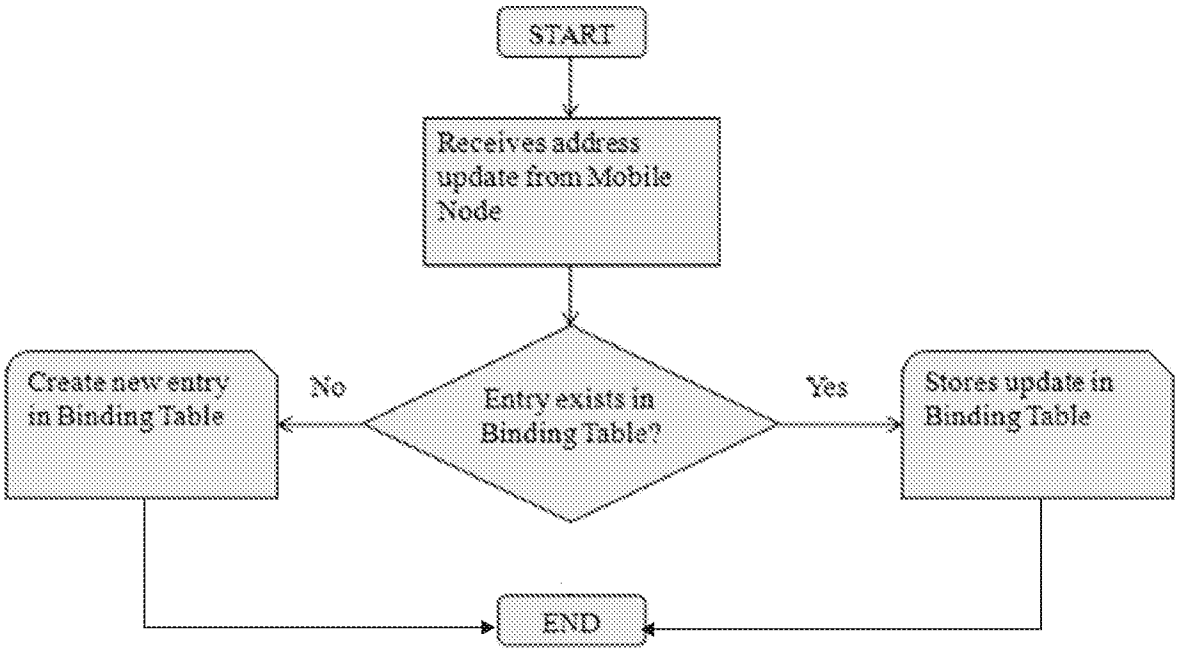
START
Receives address update from Mobile Node
Entry exists in Binding Table?
No
Yes
Create new entry in Binding Table
Stores update in Binding Table
END

FIG. 5

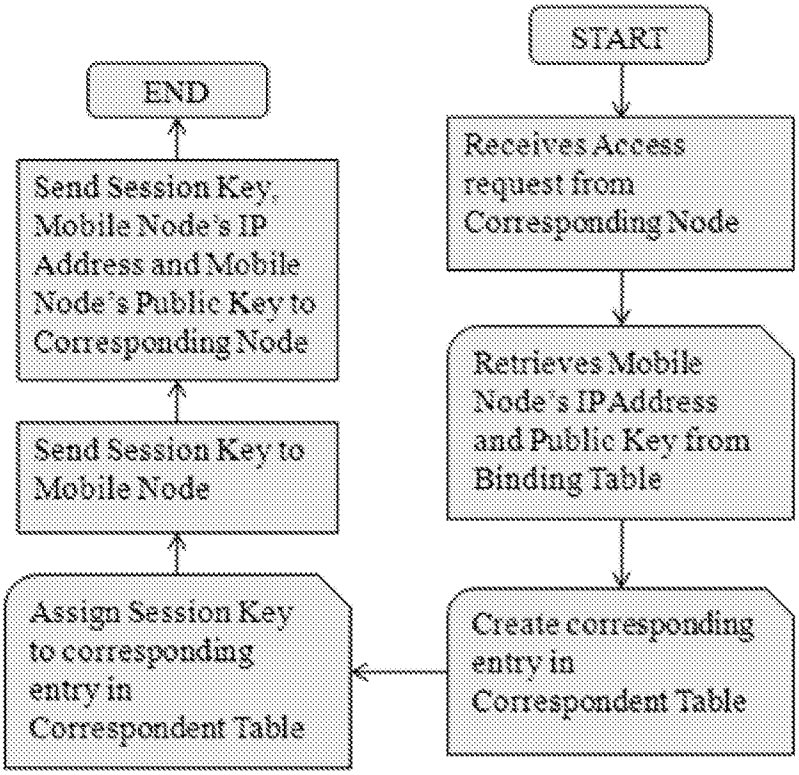
START
Receives Access request from Corresponding Node
Retrieves Mobile Node's IPAddress and Public Key from Binding Table
Create corresponding entry in Correspondent Table
Assign Session Key to corresponding entry in Correspondent Table
Send Session Key to Mobile Node
Send Session Key, Mobile Node's IP Address and Mobile Node's Public Key to Corresponding Node
END

FIG. 6

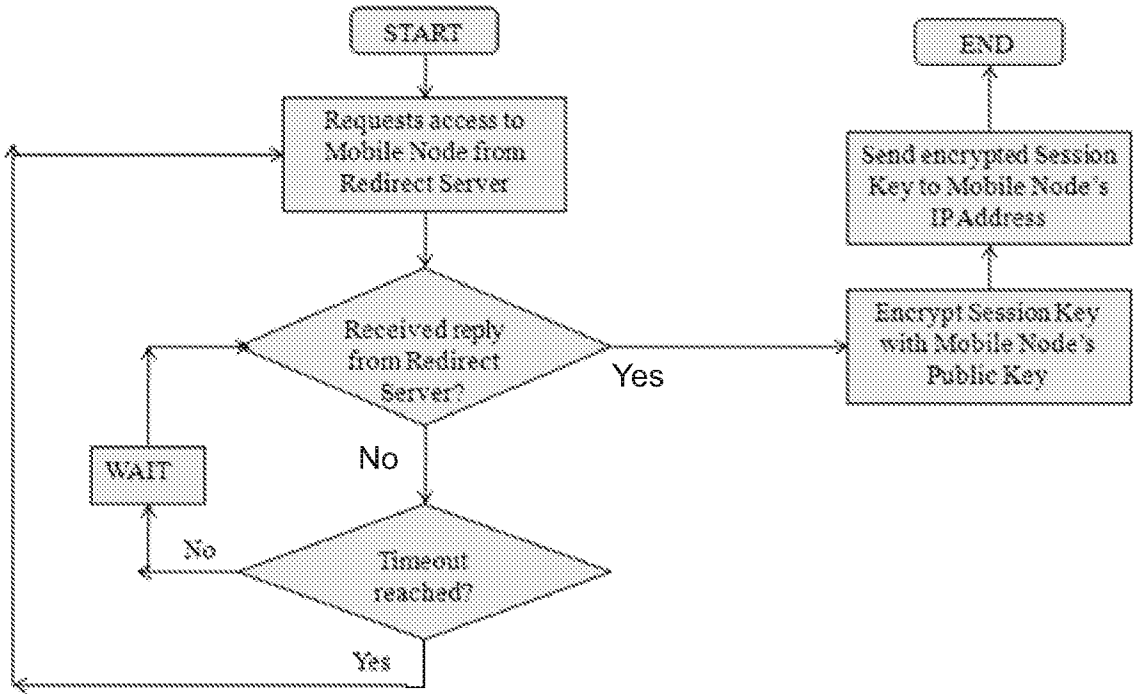
START
Requests access to Mobile Node from Redirect Server
Received reply from Redirect Server?
Yes
No
WAIT
No
Timeout reached?
Yes
Encrypt Session Key with Mobile Node's Public Key
Send encrypted Session Key to Mobile Node's IP Address
END

FIG. 7

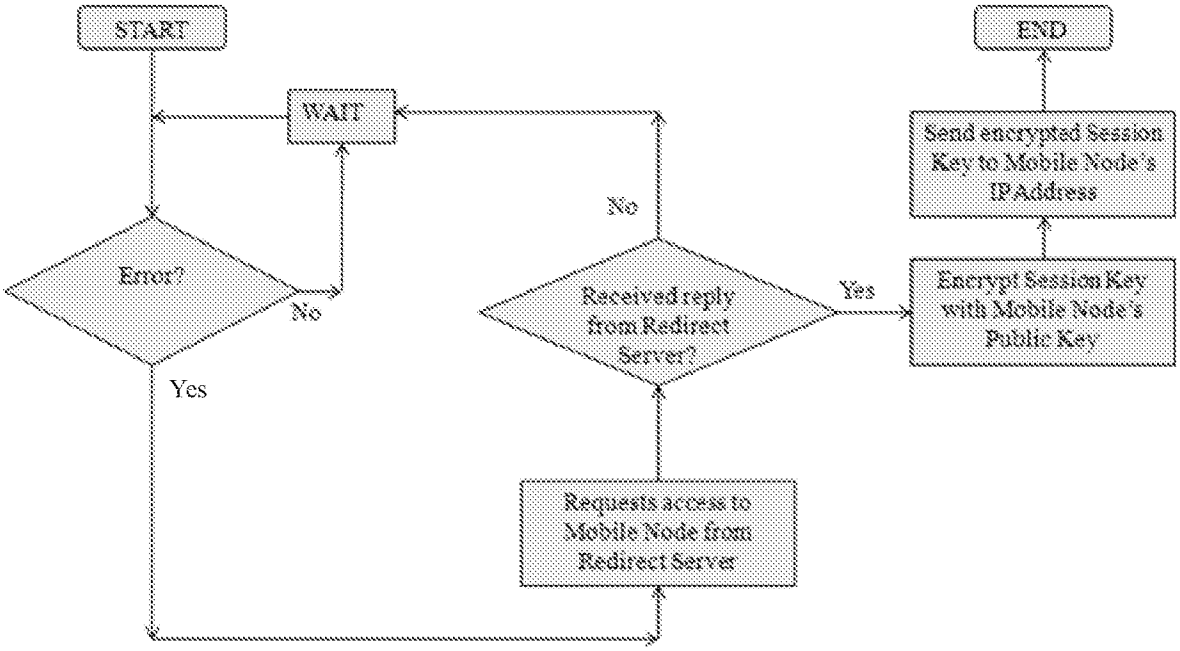
START
WAIT
Error?
No
Yes
Received reply from Redirect Server?
No
Yes
Requests access to Mobile Node from Redirect Server
Encrypt Session Key with Mobile Node's Public Key
Send encrypted Session Key to Mobile Node's IP Address
END

FIG. 8

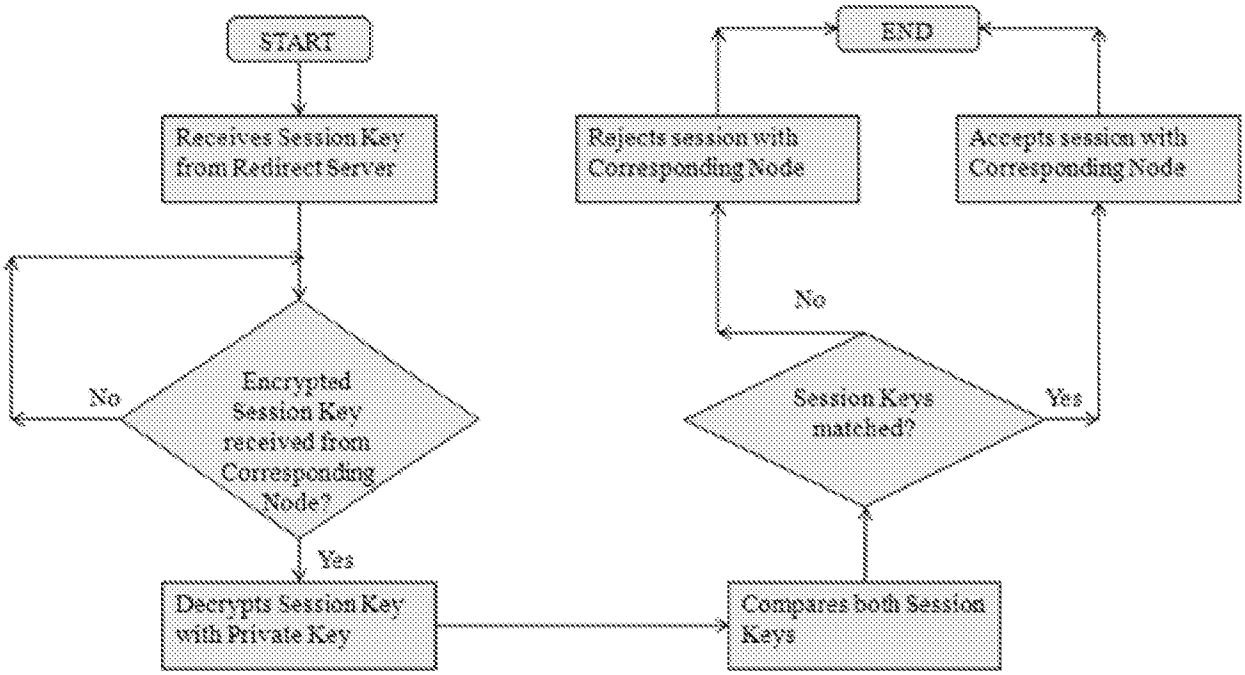
START
Receives Session Key from Redirect Server
Encrypted Session Key received from Corresponding Node?
No
Yes
Decrypts Session Key with Private Key
Compares both Session Keys
Session Keys matched?
No
Yes
Rejects session with Corresponding Node
Accepts session with Corresponding Node
END

FIG. 9

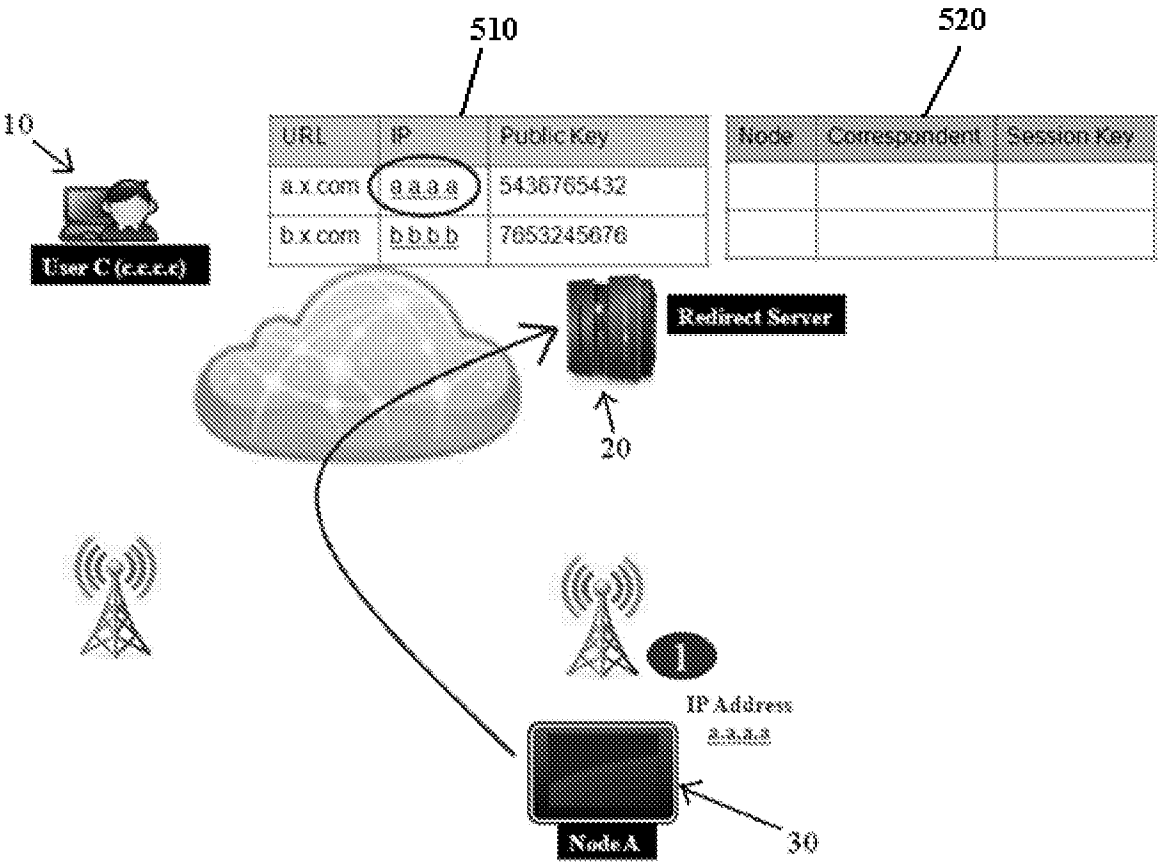
510
520
10
URL
IP
Public Key
a.x.com
a.a.a.a
5436765432
b.x.com
b.b.b.b
7853245676
Node
Correspondent
Session Key
User C (c.c.c.c)
Redirect Server
20
1
IP Address
a.a.a.a
Node A
30

FIG. 10

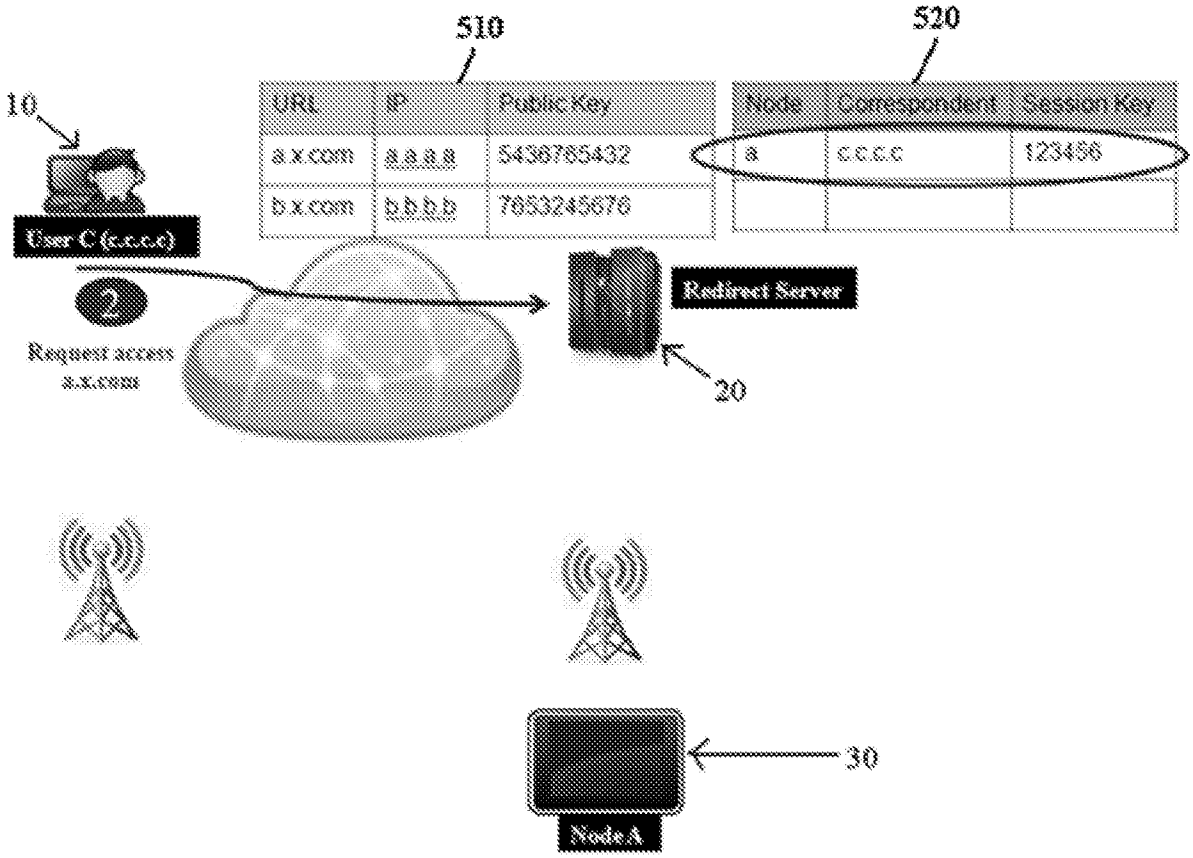
510
520
10
URL
IP
Public Key
a.x.com
a.a.a.a
5436765432
b.x.com
b.b.b.b
7653245676
Node
Correspondent
Session Key
a
c.c.c.c
123456
User C (c.c.c.c)
2
Request access a.x.com
Redirect Server
20
30
Node A

FIG. 11

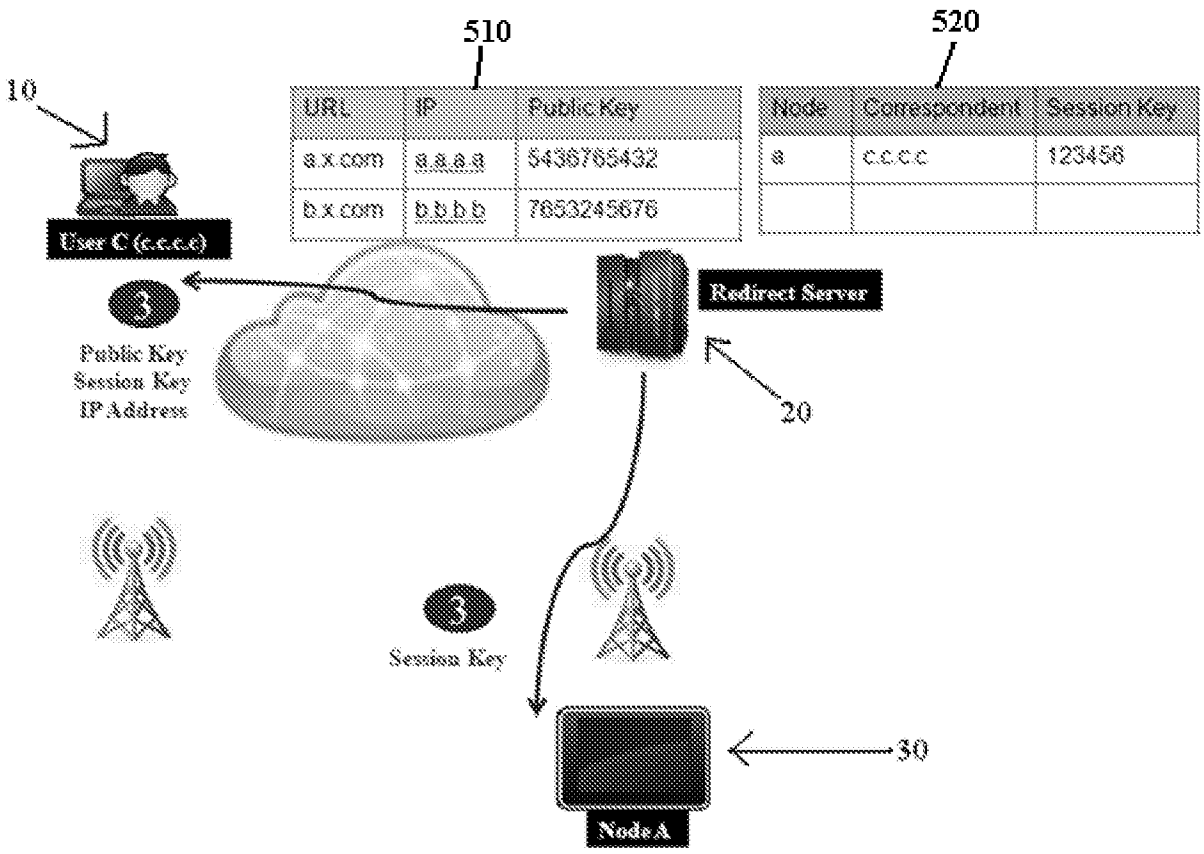
510
520
10
URL
IP
Public Key
a.x.com
a.a.a.a
5436766432
b.x.com
b.b.b.b
7653245676
Node
Correspondent
Session Key
a
c.c.c.c
123456
User C (c.c.c.c)
3
Public Key
Session Key
IP Address
Redirect Server
20
3
Session Key
30
Node A

FIG. 12

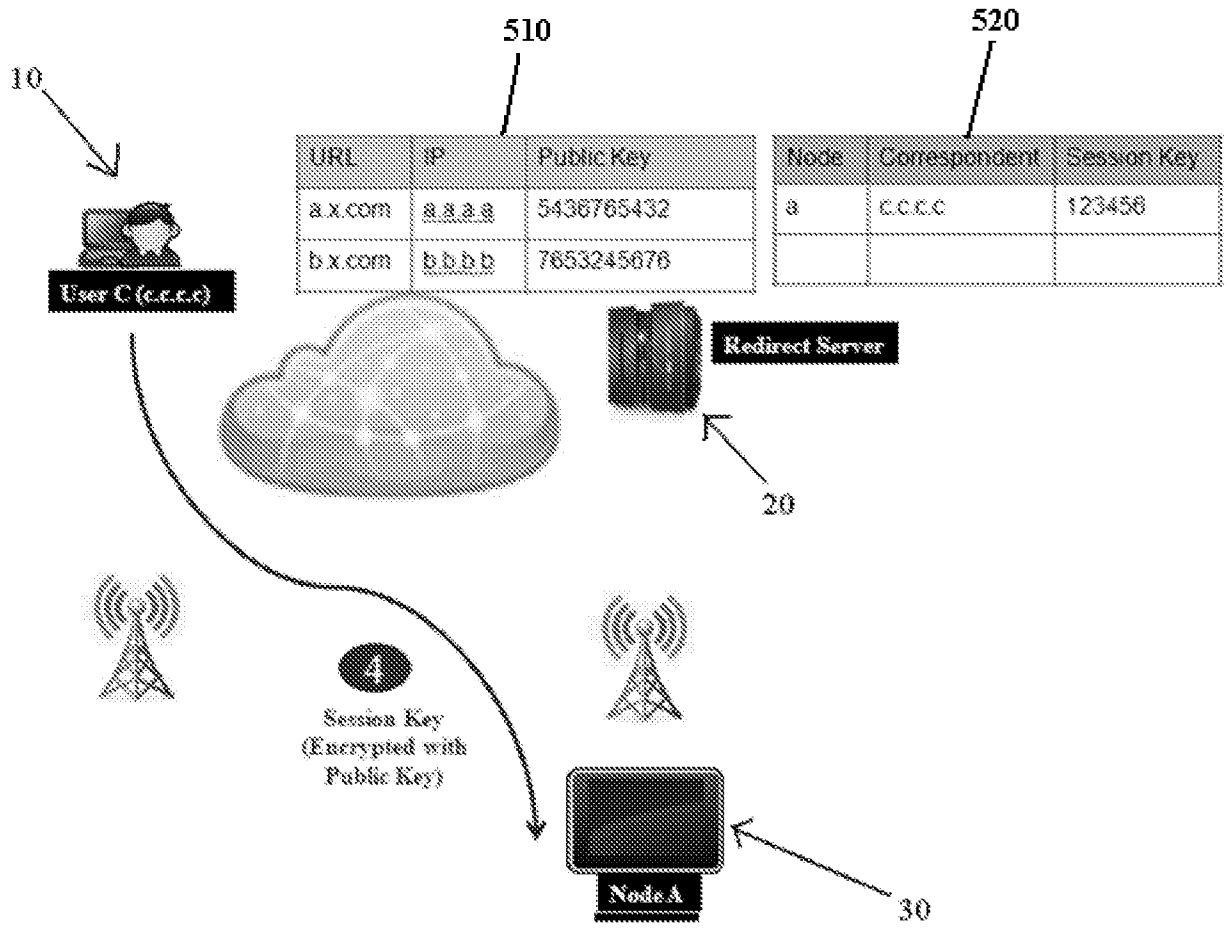
510
520
10
URL
IP
Public Key
a.x.com
a.a.a.a
5436765432
b.x.com
b.b.b.b
7653245676
Node
Correspondent
Session Key
a
c.c.c.c
123456
User C (c.c.c.c)
Redirect Server
20
4
Session Key
(Encrypted with
Public Key)
Node A
30

FIG. 13

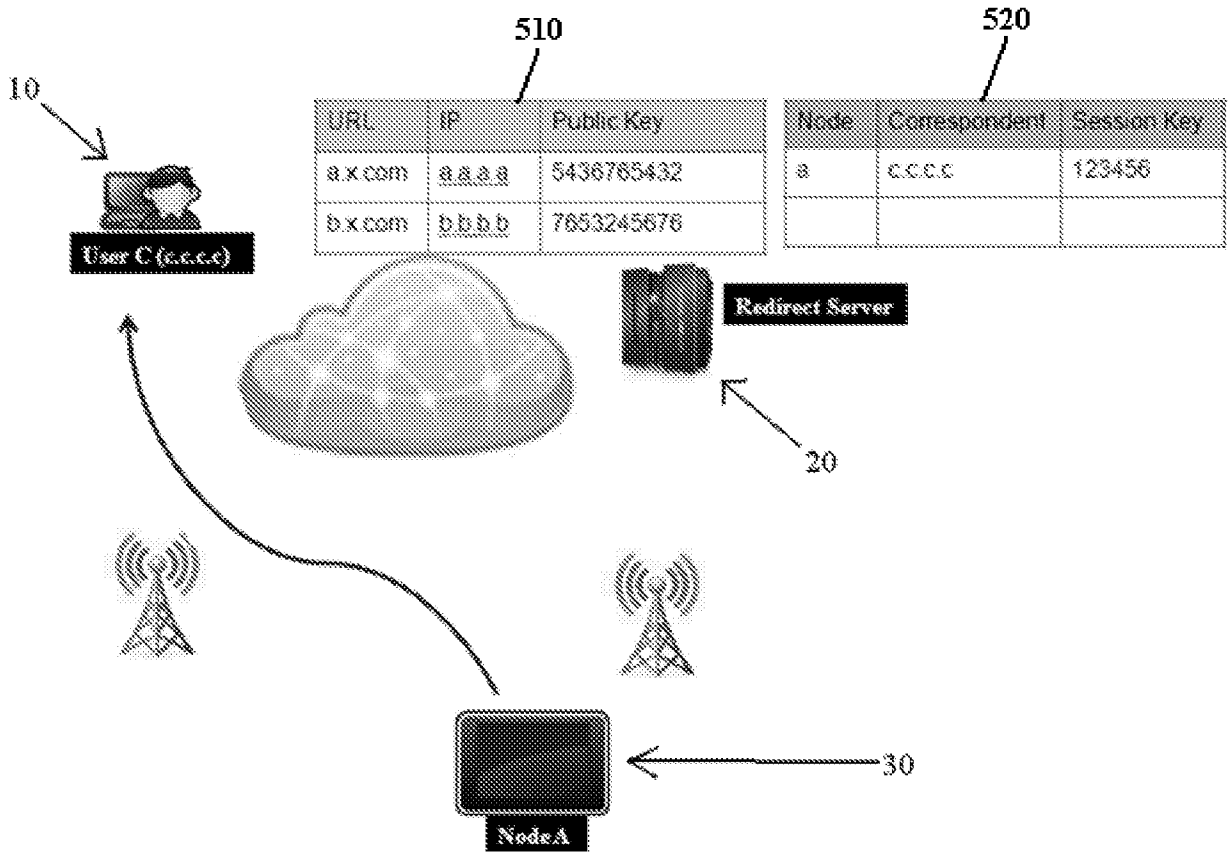
510
520
10
URL
IP
Public Key
a.x.com
a.a.a.a
5436765432
b.x.com
b.b.b.b
7653245676
Node
Correspondent
Session Key
a
c.c.c.c
123456
User C (c.c.c.c)
Redirect Server
20
30
NodeA

FIG. 14

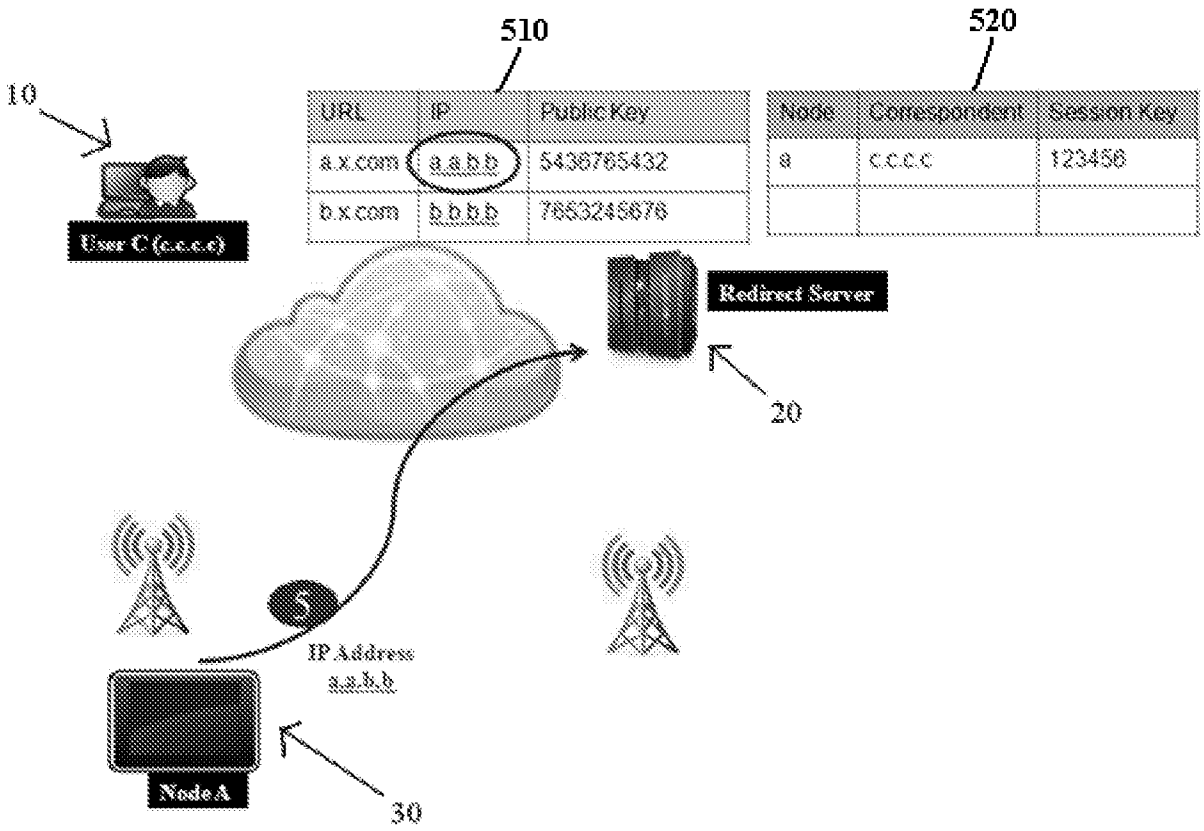
510
520
10
URL
IP
Public Key
a.x.com
a.a.b.b
5436765432
b.x.com
b.b.b.b
7653245676
Node
Correspondent
Session Key
a
c.c.c.c
123456
User C (c.c.c.c)
Redirect Server
20
5
IP Address
a.a.b.b
Node A
30

FIG. 15

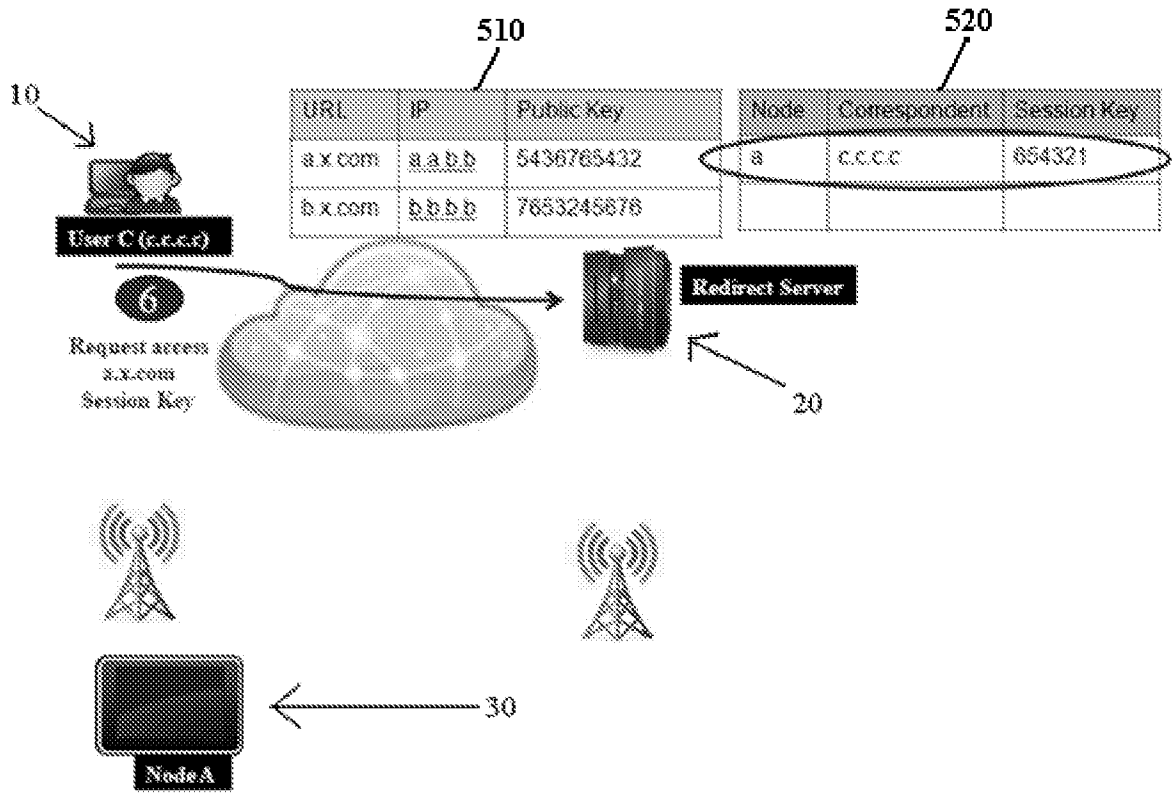
510
520
10
URL
IP
Public Key
a.x.com
a.a.b.b
5436765432
b.x.com
b.b.b.b
7653245678
Node
Correspondent
Session Key
a
c.c.c.c
654321
User C (c.c.c.c)
6
Request access
a.x.com
Session Key
Redirect Server
20
30
Node A

FIG. 16

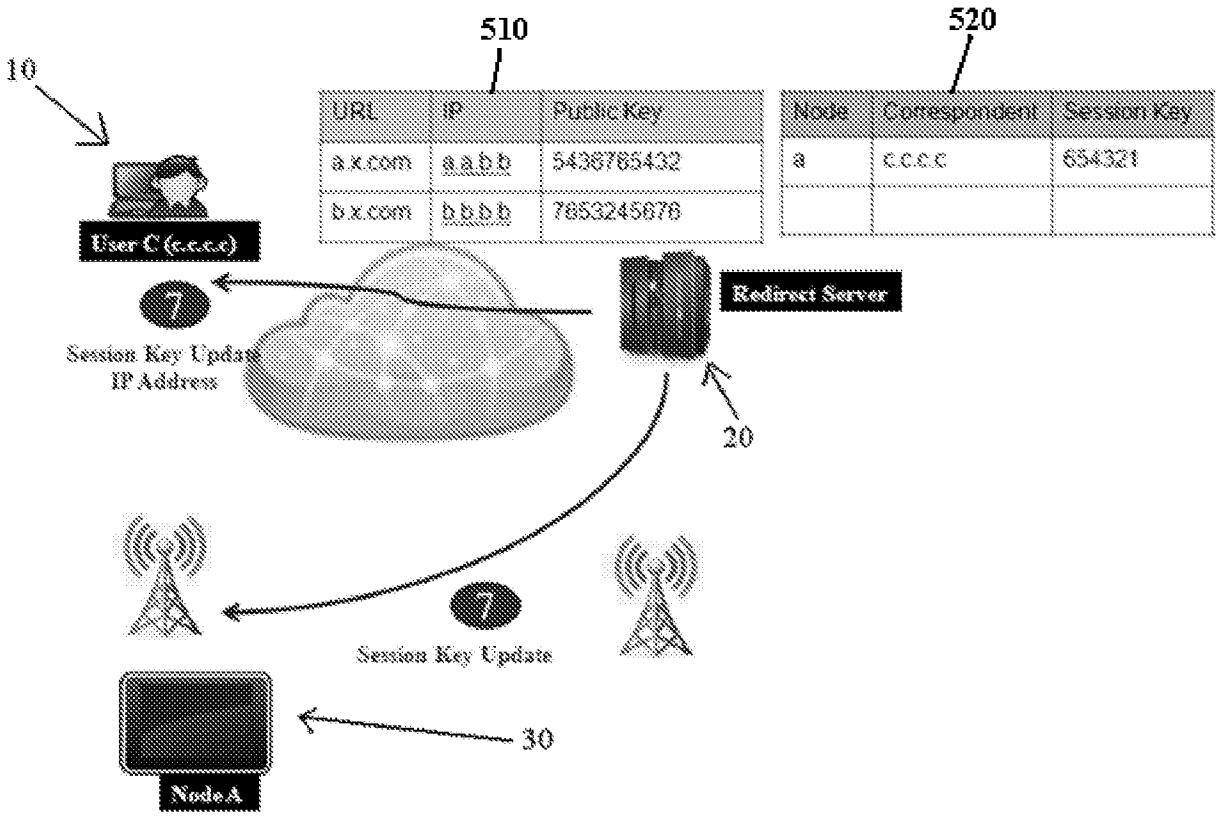
510
520
10
URL
IP
Public Key
a.x.com
a.a.b.b
5436785432
b.x.com
b.b.b.b
7853245678
Node
Correspondent
Session Key
a
c.c.c.c
654321
User C (c.c.c.c)
7
Session Key Update
IP Address
Redirect Server
20
7
Session Key Update
30
Node A

FIG. 17