



(12) **DEMANDE DE BREVET CANADIEN**
CANADIAN PATENT APPLICATION
(13) **A1**

(86) Date de dépôt PCT/PCT Filing Date: 2018/01/30 (87) Date publication PCT/PCT Publication Date: 2018/08/02 (85) Entrée phase nationale/National Entry: 2019/07/29 (86) N° demande PCT/PCT Application No.: EP 2018/052302 (87) N° publication PCT/PCT Publication No.: 2018/138381 (30) Priorité/Priority: 2017/01/30 (US62/451961)	(51) Cl.Int./Int.Cl. <i>H04W 8/06</i> (2009.01), <i>H04W 12/04</i> (2009.01), <i>H04W 36/00</i> (2009.01) (71) Demandeur/Applicant: TELEFONAKTIEBOLAGET LM ERICSSON (PUBL), SE (72) Inventeurs/Inventors: JOST, CHRISTINE, SE; TORVINEN, VESA, FI; HEDMAN, PETER, SE; CHEN, QIAN, SE; OLSSON, LARS-BERTIL, SE; BEN HENDA, NOAMEN, SE (74) Agent: ERICSSON CANADA PATENT GROUP
---	--

(54) Titre : COMMUNICATIONS SANS FIL
(54) Title: WIRELESS COMMUNICATIONS

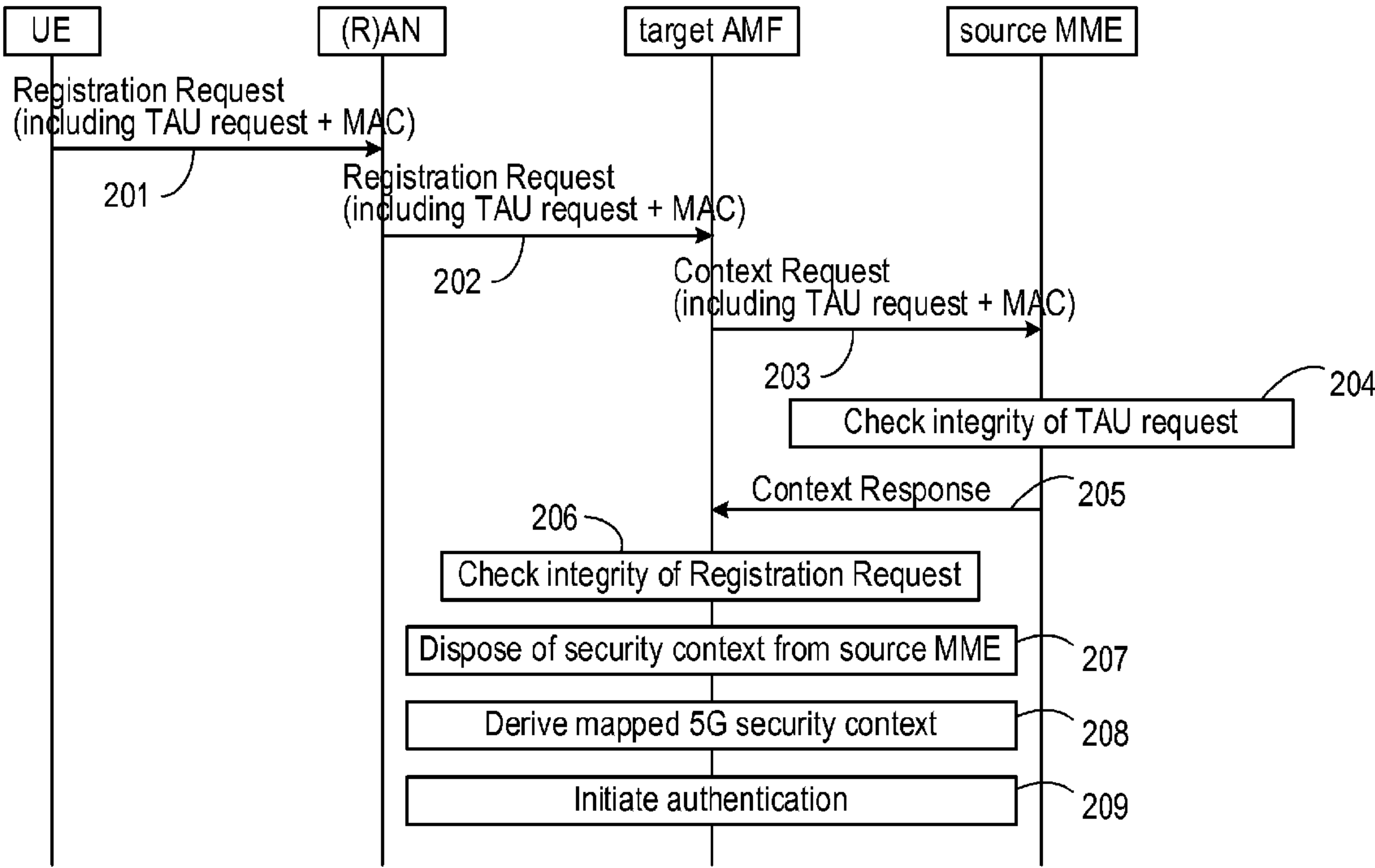


Figure 2

(57) **Abrégé/Abstract:**
A method for operating a User Equipment (UE) is disclosed, wherein the UE is served by a source first network function in a first network and requires to register with a target second network function in a second network. The method comprises generating a registration request with integrity protection for at least a part of the registration request (1200), and sending an integrity protected part of the registration request to the source first network function via the target second network function (1202). Also disclosed are methods of operating first and second network functions.

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

(19) World Intellectual Property
Organization
International Bureau

(43) International Publication Date
02 August 2018 (02.08.2018)



(10) International Publication Number
WO 2018/138381 A1

- (51) International Patent Classification:
H04W 8/06 (2009.01) H04W 36/00 (2009.01)
H04W 12/04 (2009.01)
- (21) International Application Number:
PCT/EP2018/052302
- (22) International Filing Date:
30 January 2018 (30.01.2018)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:
62/451961 30 January 2017 (30.01.2017) US
- (71) Applicant: TELEFONAKTIEBOLAGET LM
ERICSSON (PUBL) [SE/SE]; SE-164 83 Stockholm (SE).
- (72) Inventors: JOST, Christine; Västra Mårtensgatan 12,
22351 Lund (SE). TORVINEN, Vesa; Sauvontie 42, 21570
Sauvo (FI). HEDMAN, Peter; Växjögratan 7E, 252 51
HELSINGBORG (SE). CHEN, Qian; Eklanda Skog 64,
- 431 49 MÖLNDAL (SE). OLSSON, Lars-Bertil; Fjällvi-
olen 8 lgh 1301, 424 48 ANGERED (SE). BEN HENDA,
Noamen; Tumultgränd 228, 162 47 Stockholm (SE).
- (74) Agent: ERICSSON; Patent Development, Torshamnsgatan 21-23, 164 80 STOCKHOLM (SE).
- (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, 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, 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, ST, SZ, TZ,

(54) Title: WIRELESS COMMUNICATIONS

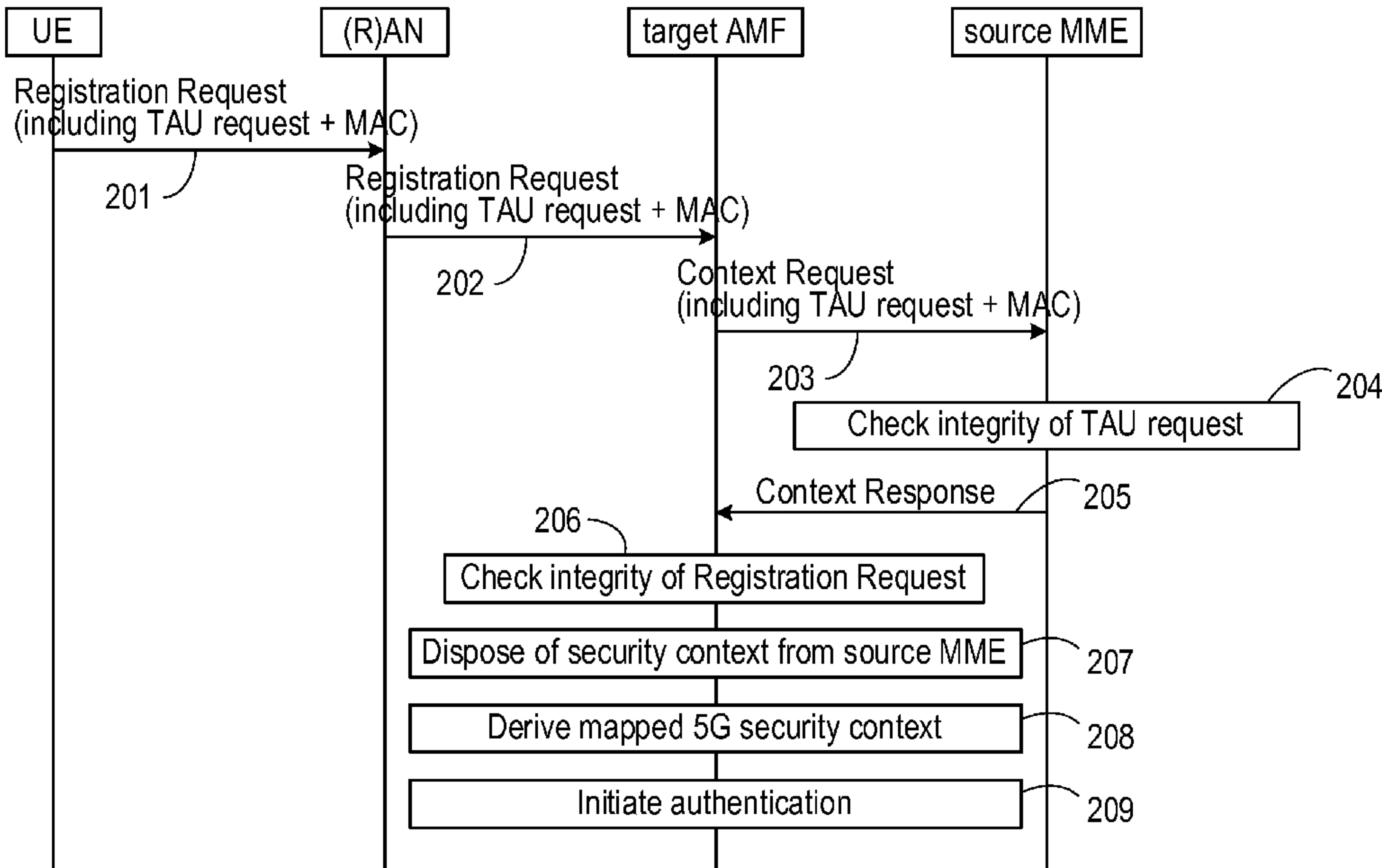


Figure 2

(57) Abstract: A method for operating a User Equipment (UE) is disclosed, wherein the UE is served by a source first network function in a first network and requires to register with a target second network function in a second network. The method comprises generating a registration request with integrity protection for at least a part of the registration request (1200), and sending an integrity protected part of the registration request to the source first network function via the target second network function (1202). Also disclosed are methods of operating first and second network functions.

WO 2018/138381 A1

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))*

WIRELESS COMMUNICATIONS**TECHNICAL FIELD**

- 5 The present disclosure relates to methods performed in a wireless communications system, and to user equipment devices and to network functions for use in such a system.

BACKGROUND

10

Currently, the 5G system is being standardized by 3GPP. It is expected that the system allows mobility from the Evolved Packet System (EPS) to the 5G system through attach or idle mode mobility. EPS uses the Tracking Area Update (TAU) procedure for location update during idle-mode mobility of the User Equipment device (UE), and the
15 Attach procedure for attach. It is expected that 5G will provide procedures for location update and attach during mobility as well. For example, the location update and attach during mobility procedures may be special cases of a more general procedure and this more general procedure may be called the registration procedure.

- 20 When a UE moves from EPS coverage to 5G coverage through reattach or idle mode mobility, it will need to send a message to notify the 5G network of this location update and/or reattach. This message may be called a registration request.

If the UE moves within the EPS, TAU requests and Attach requests sent by the UE are
25 processed in Mobility Management Entity (MME) nodes. If the UE moves within the 5G system, registration requests are processed in Access and Mobility Management Function(AMF) nodes. For interworking between EPS and the 5G system, an interface between an MME and an AMF based on the S10 interface between MMEs is expected.

30 **SUMMARY**

Aspects of the present disclosure seek to provide a mechanism for the protection of the registration request and hence mitigate against threats on the air interface such as man in the middle or replay attacks.

35

Other aspects of the present disclosure seek to provide a mechanism for a source MME to authenticate a UE on behalf of a target AMF.

According to the present invention, there is provided a method of operation of a User
5 Equipment (UE), wherein the UE is served by a source first network function in a first
network and requires to register with a target second network function in a second
network. The method comprises: generating a registration request with integrity
protection for at least a part of the registration request; and sending an integrity
protected part of the registration request to the source first network function via the
10 target second network function. The first and second network functions may be
implemented in first and second network nodes, or may be at least partially
implemented as virtualised network functions.

The first network function may be a Mobility Management Entity (MME) function, and/or
15 the second network function may be an Access and Mobility Management
Function(AMF) function.

The step of generating a registration request with integrity protection may comprise
generating a Message Authentication Code (MAC). The step of generating the
20 registration request with integrity protection may comprise generating a Message
Authentication Code (MAC) using information shared between the UE and the source
first network function. The first network function may be a Mobility Management Entity
(MME) function, and the information that is shared between the UE and the source
MME may then be at least a part of an Evolved Packet System (EPS) security context.

25 The first network function may be a Mobility Management Entity (MME) function, and
an integrity protected part of the registration request may then be an Evolved Packet
Core (EPC) Non-Access Stratum (NAS) message. The EPS NAS message may be
integrity protected with the MAC generated using information shared between the UE
30 and the source first network function. The EPC NAS message may be a Tracking Area
Update (TAU) request. The TAU request may be parsable by the source MME. The
EPC NAS message may be an Attach request. The Attach request may be parsable
by the source MME.

35 The second network function may be an Access and Mobility Management
Function(AMF) function, and the registration request may then be a 5G Non-Access

Stratum (NAS) message. The step of generating the registration request with integrity protection may comprise generating a Message Authentication Code (MAC) using information shared between the UE and a network function in the second network. The network function in the second network may be the target second network function or
5 another function in the second network. The information that is shared between the UE and a network function in the second network may be at least a part of a 5G security context. An integrity protected at least part of the registration request may be the whole registration request. The whole registration request may be integrity protected with the MAC generated using information shared between the UE and a
10 network function in the second network. The registration request may be a mobility registration request. The registration request may be an initial registration request.

The method may further comprise retrieving an EPS security context used for communication with the source first network function, deriving a mapped 5G security
15 context from the retrieved EPS security context, generating a Key Set Identifier, KSI, to identify the retrieved EPS security context, and including the KSI in the registration request.

According to the present invention, there is provided a User Equipment (UE),
20 comprising a processor and a memory, the memory containing instructions for causing the processor to perform a method comprising, when the UE is served by a source first network function in a first network and requires to register with a target second network function in a second network: generating a registration request with integrity protection for at least a part of the registration request; and sending an integrity protected part of
25 the registration request to the source first network function via the target second network function.

The first network function may be a Mobility Management Entity (MME) function, and/or the second network function may be an Access and Mobility Management
30 Function(AMF) function.

The step of generating a registration request with integrity protection may comprise generating a Message Authentication Code (MAC). The step of generating the registration request with integrity protection may comprise generating a Message
35 Authentication Code (MAC) using information shared between the UE and the source first network function. The first network function may be a Mobility Management Entity

(MME) function, and the information that is shared between the UE and the source MME may then be at least a part of an Evolved Packet System (EPS) security context.

5 The first network function may be a Mobility Management Entity (MME) function, and an integrity protected part of the registration request may then be an Evolved Packet Core (EPC) Non-Access Stratum (NAS) message. The EPS NAS message may be integrity protected with the MAC generated using information shared between the UE and the source first network function. The EPC NAS message may be a Tracking Area Update (TAU) request. The TAU request may be parsable by the source MME. The
10 EPC NAS message may be an Attach request. The Attach request may be parsable by the source MME.

The second network function may be an Access and Mobility Management Function (AMF) function, and the registration request may then be a 5G Non-Access
15 Stratum (NAS) message. The step of generating the registration request with integrity protection may comprise generating a Message Authentication Code (MAC) using information shared between the UE and a network function in the second network. The network function in the second network may be the target second network function or another function in the second network. The information that is shared between the
20 UE and a network function in the second network may be at least a part of a 5G security context. An integrity protected at least part of the registration request may be the whole registration request. The whole registration request may be integrity protected with the MAC generated using information shared between the UE and a network function in the second network. The registration request may be a mobility
25 registration request. The registration request may be an initial registration request.

The method may further comprise retrieving an EPS security context used for communication with the source first network function, deriving a mapped 5G security context from the retrieved EPS security context, generating a Key Set Identifier, KSI, to
30 identify the retrieved EPS security context, and including the KSI in the registration request.

According to the present invention, there is provided a User Equipment (UE), the UE being configured to perform the method set out above.

According to the present invention, there is provided a User Equipment (UE), comprising, for when the UE is served by a source first network function in a first network and requires to register with a target second network function in a second network: a generating module, for generating a registration request with integrity protection for at least a part of the registration request; and a sending module, for sending an integrity protected part of the registration request to the source first network function via the target second network function. The first and second network functions may be implemented in first and second network nodes, or may be at least partially implemented as virtualised network functions.

10 According to the present invention, there is provided a computer program product, containing instructions for causing a User Equipment to perform a method as set out above.

According to the present invention, there is provided a method of operation of a source first network function in a first wireless communications network. The method comprises receiving at least a part of a registration request from a User Equipment (UE) via a target second network function in a second wireless communications network, wherein the source first network function is serving the UE, and wherein the received registration request requests registration with said target second network function. The method further comprises checking integrity of the received at least part of a registration request. The first and second network functions may be implemented in first and second network nodes, or may be at least partially implemented as virtualised network functions.

25 The first network function may be a Mobility Management Entity (MME) function, and/or the second network function may be an Access and Mobility Management Function(AMF) function.

The step of checking the integrity may comprise generating a Message Authentication Code (MAC). The step of checking the integrity may comprise generating the Message Authentication Code (MAC) using information shared between the UE and the source first network function. The first network function may be a Mobility Management Entity (MME) function, and the information that is shared between the UE and the source MME may then be at least part of an Evolved Packet System (EPS) security context.

The first network function may be a Mobility Management Entity (MME) function, and the integrity protected part of the registration request may then be an Evolved Packet Core (EPC) Non-Access Stratum (NAS) message. The EPC NAS message may be a Tracking Area Update (TAU) request. The TAU request may be parsable by the
5 source MME. The EPC NAS message may be an Attach request. The Attach request may be parsable by the source MME.

The second network function may be an Access and Mobility Management Function(AMF) function, and the registration request may then be a 5G Non-Access
10 Stratum (NAS) message. The integrity protected at least part of the registration request may be the whole registration request. The registration request may be a mobility registration request. The registration request may be an initial registration request.

15 The method may further comprise, in response to the received at least part of a registration request passing the integrity check, providing user information to the target second network function. The method may further comprise, in response to the received at least part of a registration request failing the integrity check, notifying the second network function that the UE may not be authenticated.

20

According to the present invention, there is provided apparatus for implementing a first network function for use in a first wireless communications network, the apparatus comprising a processor and a memory, the memory containing instructions for causing the processor to perform a method comprising: receiving at least a part of a registration
25 request from a User Equipment (UE) via a target second network function in a second wireless communications network, wherein the source first network function is serving the UE, and wherein the received registration request requests registration with said target second network function, the method comprising: checking integrity of the received at least part of a registration request. The apparatus may for example
30 comprise a network node and may comprise a plurality of network nodes. The first and second network functions may be implemented in first and second network nodes, or may be at least partially implemented as virtualised network functions.

The first network function may be a Mobility Management Entity (MME) function, and/or the second network function may be an Access and Mobility Management
35 Function(AMF) function.

The step of checking the integrity may comprise generating a Message Authentication Code (MAC). The step of checking the integrity may comprise generating the Message Authentication Code (MAC) using information shared between the UE and the source first network function. The first network function may be a Mobility Management Entity (MME) function, and the information that is shared between the UE and the source MME may then be at least part of an Evolved Packet System (EPS) security context.

The first network function may be a Mobility Management Entity (MME) function, and the integrity protected part of the registration request may then be an Evolved Packet Core (EPC) Non-Access Stratum (NAS) message. The EPC NAS message may be a Tracking Area Update (TAU) request. The TAU request may be parsable by the source MME. The EPC NAS message may be an Attach request. The Attach request may be parsable by the source MME.

The second network function may be an Access and Mobility Management Function (AMF) function, and the registration request may then be a 5G Non-Access Stratum (NAS) message. The integrity protected at least part of the registration request may be the whole registration request. The registration request may be a mobility registration request. The registration request may be an initial registration request.

The method may further comprise, in response to the received at least part of a registration request passing the integrity check, providing user information to the target second network function. The method may further comprise, in response to the received at least part of a registration request failing the integrity check, notifying the second network function that the UE may not be authenticated.

According to the present invention, there is provided apparatus for implementing a first network function, the apparatus being configured to perform a method as set out above. The apparatus may for example comprise a network node and may comprise a plurality of network nodes.

According to the present invention, there is provided apparatus for implementing a first network function for use in a first wireless communications network. The apparatus comprises: a receiving module for receiving at least a part of a registration request from a User Equipment (UE) via a target second network function in a second wireless

communications network, wherein the source first network function is serving the UE, and wherein the received registration request requests registration with said target second network function. The apparatus further comprises a checking module for checking integrity of the received at least part of a registration request. The apparatus
5 may for example comprise a network node and may comprise a plurality of network nodes. The first and second network functions may be implemented in first and second network nodes, or may be at least partially implemented as virtualised network functions.

According to the present invention, there is provided a computer program product,
10 containing instructions for causing a first network function to perform a method in as set out above.

According to the present invention, there is provided a method of operation of a second network function in a second network. The method comprises: receiving a
15 registration request from a User Equipment (UE); and forwarding a request to retrieve information about the UE to a first network function in a first network serving the UE. The first and second network functions may be implemented in first and second network nodes, or may be at least partially implemented as virtualised network functions.

20 The second network function may be an Access and Mobility Management Function(AMF) function, and/or the first network function may be a Mobility Management Entity (MME) function.

The method may comprise receiving the registration request from the User Equipment
25 (UE) via an access network.

The request to retrieve information about the UE may comprise a context request. The first network function may be a Mobility Management Entity (MME) function, and the context request may then comprise a Tracking Area Update Request from the
30 registration request. The first network function may be a Mobility Management Entity (MME) function, and the context request may then comprise the whole registration request.

The request to retrieve information about the UE may comprise an identification
35 request. The first network function may be a Mobility Management Entity (MME) function, and the identification request may then comprise an Attach Request from the

registration request. The first network function may be a Mobility Management Entity (MME) function, and the identification request may then comprise the whole registration request.

- 5 The request to retrieve information about the UE may comprise at least a part of the registration request, and said part of the registration request may be integrity protected.

The second network function may be an Access and Mobility Management Function(AMF) function and the first network function may be a Mobility Management
10 Entity (MME) function and said part of the registration request may be integrity protected using an EPS security context.

The second network function may be an Access and Mobility Management Function(AMF) function and the first network function may be a Mobility Management
15 Entity (MME) function and the registration request may be integrity protected using a 5G security context. The method may further comprise checking the integrity of the received registration request.

The step of checking the integrity may comprise generating a Message Authentication
20 Code (MAC) using the 5G security context.

The method may further comprise, in response to the received registration request passing the integrity check, discarding a response received from the first network function to the request to retrieve information.

25

The method may further comprise, in response to the received registration request failing the integrity check, performing at least one of: deriving a mapped 5G security context from an EPS security context received from the first function in response to the request to retrieve information; or initiating an authentication procedure to create a new
30 5G security context.

The method may further comprise determining that the 5G security context used to integrity protect the registration request is unavailable, and performing at least one of: deriving a mapped 5G security context from an EPS security context received from the
35 first function in response to the request to retrieve information; or initiating an authentication procedure to create a new 5G security context.

- The second network function may be an Access and Mobility Management Function(AMF) function and the first network function may be a Mobility Management Entity (MME) function, and the registration request may include a Key Set Identifier, KSI. The method may further comprise using the KSI to identify an EPS security context from a response received from the first function to the request to retrieve information, and deriving a mapped 5G security context from the identified EPS security context.
- 10 According to the present invention, there is provided apparatus for implementing a second network function for use in a second wireless communications network, the apparatus comprising a processor and a memory, the memory containing instructions for causing the processor to perform a method comprising: receiving a registration request from a User Equipment (UE); and forwarding a request to retrieve information about the UE to a first network function in a first network serving the UE. The apparatus may for example comprise a network node and may comprise a plurality of network nodes. The first and second network functions may be implemented in first and second network nodes, or may be at least partially implemented as virtualised network functions.
- 20 The second network function may be an Access and Mobility Management Function(AMF) function, and/or the first network function may be a Mobility Management Entity (MME) function.
- 25 The method may comprise receiving the registration request from the User Equipment (UE) via an access network.
- The request to retrieve information about the UE may comprise a context request. The first network function may be a Mobility Management Entity (MME) function, and the context request may then comprise a Tracking Area Update Request from the registration request. The first network function may be a Mobility Management Entity (MME) function, and the context request may then comprise the whole registration request.
- 30 The request to retrieve information about the UE may comprise an identification request. The first network function may be a Mobility Management Entity (MME)

function, and the identification request may then comprise an Attach Request from the registration request. The first network function may be a Mobility Management Entity (MME) function, and the identification request may then comprise the whole registration request.

5

The request to retrieve information about the UE may comprise at least a part of the registration request, and said part of the registration request may be integrity protected.

10 The second network function may be an Access and Mobility Management Function(AMF) function and the first network function may be a Mobility Management Entity (MME) function and said part of the registration request may be integrity protected using an EPS security context.

15 The second network function may be an Access and Mobility Management Function(AMF) function and the first network function may be a Mobility Management Entity (MME) function and the registration request may be integrity protected using a 5G security context. The method may further comprise checking the integrity of the received registration request.

20 The step of checking the integrity may comprise generating a Message Authentication Code (MAC) using the 5G security context.

25 The method may further comprise, in response to the received registration request passing the integrity check, discarding a response received from the first network function to the request to retrieve information.

30 The method may further comprise, in response to the received registration request failing the integrity check, performing at least one of: deriving a mapped 5G security context from an EPS security context received from the first function in response to the request to retrieve information; or initiating an authentication procedure to create a new 5G security context.

35 The method may further comprise determining that the 5G security context used to integrity protect the registration request is unavailable, and performing at least one of: deriving a mapped 5G security context from an EPS security context received from the

first function in response to the request to retrieve information; or initiating an authentication procedure to create a new 5G security context.

The second network function may be an Access and Mobility Management Function(AMF) function and the first network function may be a Mobility Management Entity (MME) function, and the registration request may include a Key Set Identifier, KSI. The method may further comprise using the KSI to identify an EPS security context from a response received from the first function to the request to retrieve information, and deriving a mapped 5G security context from the identified EPS security context.

According to the present invention, there is provided apparatus for implementing a second network function for use in a second wireless communications network, the apparatus being configured for performing a method in accordance with any of the methods set out above. The apparatus may for example comprise a network node and may comprise a plurality of network nodes. The first and second network functions may be implemented in first and second network nodes, or may be at least partially implemented as virtualised network functions.

According to the present invention, there is provided apparatus for implementing a second network function for use in a second wireless communications network, the apparatus comprising: a receiving module for receiving a registration request from a User Equipment (UE); and a forwarding module for forwarding a request to retrieve information about the UE to a first network function in a first network serving the UE. The apparatus may for example comprise a network node and may comprise a plurality of network nodes. The first and second network functions may be implemented in first and second network nodes, or may be at least partially implemented as virtualised network functions.

According to the present invention, there is provided a computer program product, containing instructions for causing a second network function to perform a method in accordance with any one of the methods set out above.

BRIEF DESCRIPTION OF THE DRAWINGS

35

Figure 1 illustrates a part of a wireless communications system.

Figure 2 is a signalling diagram illustrating a first procedure.

Figure 3 is a signalling diagram illustrating a second procedure.

5

Figure 4 is a signalling diagram illustrating a third procedure.

Figure 5 is a signalling diagram illustrating a fourth procedure.

10 Figure 6 is a block diagram illustrating a user equipment device.

Figure 7 is a block diagram illustrating a user equipment device.

15 Figure 8 is a block diagram illustrating apparatus for implementing a first network function.

Figure 9 is a block diagram illustrating apparatus for implementing a first network function.

20 Figure 10 is a block diagram illustrating apparatus for implementing a second network function.

Figure 11 is a block diagram illustrating apparatus for implementing a second network function.

25

Figure 12 is a flow chart, illustrating a procedure performed in a user equipment device.

Figure 13 is a flow chart, illustrating a procedure performed in a first network function.

30 Figure 14 is a flow chart, illustrating a procedure performed in a second network function.

DETAILED DESCRIPTION

35 Aspects and examples of the disclosure are described with reference to EPS and 5G networks but it will be appreciated that they may be applicable to other networks.

Figure 1 illustrates a part of a wireless communications system, comprising a first network function in a first network, and a second network function in a second network. In this illustrated example, the first network function is a Mobility Management Entity (MME) function 110, and the first network is an Evolved Packet System (EPS) network. Further, in this example, the second network function is an Access and Mobility Management Function (AMF) function 120, and the second network is a 5G network. Thus, the first network and the second network use different technologies or standards, but are managed by the same network operator and appear to the consumer as part of the same network. This illustrated example is used as the basis for further explanation below, but the methods described herein may be used for the interoperation of any two such networks. The first and second network functions may be implemented in first and second network nodes, or may be at least partially implemented as virtualised network functions.

In this example, there is an interface 130 between the first network function and the second network function. Specifically, in this illustrated example where the first network function is a Mobility Management Entity (MME) 110, and the second network function is an Access and Mobility Management Function (AMF) 120, the interface 130 can be the S10 interface or a modified version of the S10 interface.

Figure 1 shows a user equipment device (UE) 140 that obtains service from the wireless communications network. The term user equipment device (UE) is used herein to refer to any terminal device, whether that device is intended to be a user-operated device such as a smartphone, tablet or laptop computer, or the like, or whether that device is intended to operate independently, for example as a remote sensor of the like. Similarly, the UE may be intended to operate from a generally fixed location, for example in the case of a closed-circuit TV camera or the like, or may be intended to be mobile, for example in the case of a smartphone, tablet or laptop computer, tracking device, or the like.

The UE 140 connects to the first network function and the second network function through one or more functions or nodes of one or more access networks (AN) 150, which may for example include a radio access network (RAN). Any suitable radio access technology may be used for enabling the connection of the UE 140 to the first network function and the second network function.

Figure 2 is a signalling diagram illustrating a first procedure in the example where the first network function is a Mobility Management Entity (MME), and the second network function is an Access and Mobility Management Function(AMF).

5

Specifically, Figure 2 illustrates a procedure where a UE is being served by a source MME, but requires to register with a target AMF. More specifically, Figure 2 illustrates a procedure where the registration is based on location update, including a tracking area update (TAU).

10

In step 201, the UE sends to the Radio Access Network a Registration Request. This contains information indicating that the Registration type is mobility registration, and a Temporary User ID for the UE indicating an identity of the source MME. The Registration Request may optionally also contain parameters that the MME can parse.

15

Such parameters can for example include the EPS UE Core Network Capability, the EPS key set identifier, and/or the EPC Non Access Stratum (NAS) sequence number. The Registration Request may optionally also contain parameters that the MME cannot parse. Such parameters can for example include the UE 5G Core Network (5GCN) Capability, and/or a 5G parameter to support network slice selection (for example NSSAI).

20

In addition, the UE also constructs a legacy TAU Request that the source MME would be able to parse. The TAU Request contains all the parameters from the Registration Request that the MME can parse and also includes a genuine EPS Globally Unique Temporary ID (GUTI). In some examples, the UE may not construct a full TAU message, but may include only sufficient Information Elements to enable the AMF to create a protected TAU for sending to the MME for verification (see below).

25

More generally, the UE can send any message (for use in any second network), with a message format that makes use of the legacy security header and related parameters (in this example the NAS security header and related parameters). The NAS security header and additional security parameters can then be used by the source MME to validate the checksum in MAC. In other respects, the message from the UE may be of an arbitrary format.

30

35

The UE integrity protects at least a part of the Registration Request. In some examples, the UE integrity protects an Extended Packet System (EPS) Non Access Stratum (NAS) message. More specifically, in this example, the UE integrity protects the TAU Request. Specifically, the UE may integrity protect the TAU Request with a Message Authentication Code (MAC). The MAC may be computed with at least a part of the Extended Packet System (EPS) security context matching the one that is stored in the source MME. For example, the security context may contain keys to be used for encryption and for integrity protection, but in some examples only the keys for integrity protection are used in computing the MAC.

Thus, in step 201, the UE sends to the Radio Access Network the Registration Request, the TAU Request, and the MAC included in the TAU Request.

In step 202, the RAN forwards the received Registration Request, also including the TAU Request, and the MAC included in the TAU Request, to the target AMF.

In step 203, the target AMF sends a message to the source MME to request user information relating to the UE. In some examples, the message requesting UE information is a Context Request message. In some examples, the Context Request message includes the complete integrity protected TAU Request message, and other parameters, for example such as the Globally Unique Temporary ID (GUTI) and/or a MME address.

In step 204, the source MME receives the Context Request message, and checks the integrity of the integrity protected part of the received message. For example, in the cases described above, the source MME computes a MAC for the TAU Request. The MAC is computed with the same part of the Extended Packet System (EPS) security context that is used by the UE. The MME may use the EPS GUTI to find the UE context including the security context for computing the MAC.

Thus, the source MME is able to check that the MAC that it computes is identical to the MAC contained in the received Context Request message. If so, the source MME can confirm that the message has not been tampered with.

If the source MME determines that the message has not been tampered with, it sends the requested user information to the target AMF in response to the Context Request message in step 205.

- 5 If the source MME determines that the integrity check is failed, and hence that the message has potentially been tampered with, it may still send the requested user information to the target AMF in step 205, but it will indicate that the UE could not be authenticated. The failed authentication can be used by the target system as a trigger to authenticate the UE in order to establish new security keys (since the user could not
10 be authenticated using the existing security keys).

In some examples, when constructing the legacy message, such as the legacy TAU message for including in the Registration Request to the RAN, the UE may use the EPS security context matching the one that is stored in the source MME to derive a
15 mapped 5G security context. The UE may also generate a Key Set Identifier (KSI), such as a ngKSI, to identify the EPS security context used for deriving the mapped 5G security context, and may include the generated KSI in the Registration Request message. The UE may also in some examples include UE 5G security capabilities in the Registration Request message.

20

On receipt of the context response message from the source MME in step 205, the target AMF may use the KSI included in the Registration Request message to identify the EPS security context that was used by the UE to derive a mapped 5G security context, from the EPS security context information included in the context response
25 message. The AMF may then derive the same mapped 5G security context in step 208.

In further examples, the UE may have stored a native 5G security context, in addition to an EPS security context. Such a native 5G security context may for example have
30 been established during an earlier connection to the 5G network. In such examples, the UE may include its 5G security capabilities and an appropriate ngKSI in the Registration Request message. The UE may integrity protect the entire Registration Request message using the native 5G security context. This integrity protection of the entire Registration Request message using a 5G security context may be in addition to
35 the integrity protection of the legacy message included in the Registration Request message using the EPS security context. The integrity protection of the entire

Registration Request message may be conducted by using at least a part of the 5G security context to calculate a MAC and including the MAC with the Registration Request message.

- 5 The AMF may verify the integrity of the Registration Request message using the 5G security context at step 206. If the verification is successful, the AMF may, at step 207, dispose of any security parameters received from the source MME in the Context Response message. If the verification fails or the 5G UE context is not available to allow verification to take place, the AMF may then treat the Registration request
- 10 message as unprotected. In such cases, the AMF may either derive a mapped 5G security context in step 208 from the EPS context received from the source MME in the Context Response message, or the AMF may initiate an authentication procedure to create a new native 5G security context in step 209. The AMF may then activate the resulting security context (mapped or native) by a NAS SMC procedure.

15

Figure 3 is a signalling diagram illustrating a second procedure in the example where the first network function is a Mobility Management Entity (MME), and the second network function is an Access and Mobility Management Function(AMF).

- 20 Specifically, Figure 3 illustrates a procedure where a UE is being served by a source MME, but requires to register with a target AMF. More specifically, Figure 3 illustrates a procedure where the registration is based on attach.

- 25 In step 301, the UE sends to the Radio Access Network a Registration Request. This contains information indicating that the Registration type is an initial registration, and a Temporary User ID for the UE indicating an identity of the source MME. The Registration Request may optionally also contain parameters that the MME can parse. Such parameters can for example include the EPS UE Core Network Capability, the EPS key set identifier, and/or the EPC Non Access Stratum (NAS) sequence number.
- 30 The Registration Request may optionally also contain parameters that the MME cannot parse. Such parameters can for example include the UE 5G Core Network (5GCN) Capability, and/or a 5G parameter to support network slice selection (for example NSSAI).

In addition, the UE also constructs a legacy Attach Request that the source MME would be able to parse. The Attach Request contains some or all of the parameters from the Registration Request that the MME can parse.

- 5 More generally, the UE can send any message (for use in any second network), with a message format that makes use of the legacy security header and related parameters (in this example the NAS security header and related parameters). The NAS security header and additional security parameters can then be used by the source MME to validate the checksum in MAC. In other respects, the message from the UE may be of
10 an arbitrary format.

- The UE integrity protects at least a part of the Registration Request. In some examples, the UE integrity protects an Extended Packet System (EPS) Non Access Stratum (NAS) message. More specifically, in this example, the UE integrity protects
15 the Attach Request. Specifically, the UE may integrity protect the Attach Request with a Message Authentication Code (MAC). The MAC may be computed with at least a part of the Extended Packet System (EPS) security context matching the one that is stored in the source MME. For example, the security context may contain keys to be used for encryption and for integrity protection, but in some examples only the keys for
20 integrity protection are used in computing the MAC.

Thus, in step 301, the UE sends to the Radio Access Network the Registration Request, the Attach Request, and the MAC included in the Attach Request.

- 25 In step 302, the RAN forwards the received Registration Request, also including the Attach Request, and the MAC included in the Attach Request, to the target AMF.

- In step 303, the target AMF sends a message to the source MME to request user information relating to the UE. In some examples, the message requesting UE
30 information is an Identification Request message. In some examples, the Identification Request message includes the complete integrity protected Attach Request message, and other parameters, for example such as an old Globally Unique Temporary ID (GUTI).

- 35 In step 304, the source MME receives the Identification Request message, and checks the integrity of the integrity protected part of the received message. For example, in

the cases described above, the source MME computes a MAC for the Attach Request. The MAC is computed with the same part of the Extended Packet System (EPS) security context that is used by the UE.

- 5 Thus, the source MME is able to check that the MAC that it computes is identical to the MAC contained in the received Identification Request message. If so, the source MME can confirm that the message has not been tampered with.

- 10 If the source MME determines that the message has not been tampered with, it sends the requested user information to the target AMF in response to the Identification Request message in step 305.

- 15 If the source MME determines that the integrity check is failed, and hence that the message has potentially been tampered with, it will indicate that the UE could not be authenticated, and it may not send any security related information to the target AMF in step 305. The failed authentication can be used by the target system as a trigger to authenticate the UE in order to establish new security keys (since the user could not be authenticated using the existing security keys).

- 20 In some examples, when constructing the legacy message, such as the legacy attach message for including in the Registration Request to the RAN, the UE may use the EPS security context matching the one that is stored in the source MME to derive a mapped 5G security context. The UE may also generate a Key Set Identifier (KSI), such as a ngKSI, to identify the EPS security context used for deriving the mapped 5G security context, and may include the generated KSI in the Registration Request message. The UE may also in some examples include UE 5G security capabilities in the Registration Request message.

- 30 On receipt of the context response message from the source MME in step 305, the target AMF may use the KSI included in the Registration Request message to identify the EPS security context that was used by the UE to derive a mapped 5G security context, from the EPS security context information included in the context response message. The AMF may then derive the same mapped 5G security context in step 308.

In further examples, the UE may have stored a native 5G security context, in addition to an EPS security context. Such a native 5G security context may for example have been established during an earlier connection to the 5G network. In such examples, the UE may include its 5G security capabilities and an appropriate ngKSI in the

5 Registration Request message. The UE may integrity protect the entire Registration Request message using the native 5G security context. This integrity protection of the entire Registration Request message using a 5G security context may be in addition to the integrity protection of the legacy message included in the Registration Request message using the EPS security context. The integrity protection of the entire

10 Registration Request message may be conducted by using at least a part of the 5G security context to calculate a MAC and including the MAC with the Registration Request message.

The AMF may verify the integrity of the Registration Request message using the 5G

15 security context at step 306. If the verification is successful, the AMF may, at step 307, dispose of any security parameters received from the source MME in the Context Response message. If the verification fails or the 5G UE context is not available to allow verification to take place, the AMF may then treat the Registration request message as unprotected. In such cases, the AMF may either derive a mapped 5G

20 security context in step 308 from the EPS context received from the source MME in the Context Response message, or the AMF may initiate an authentication procedure to create a new native 5G security context in step 309. The AMF may then activate the resulting security context (mapped or native) by a NAS SMC procedure.

25 Figure 4 is a signalling diagram illustrating a third procedure in the example where the first network function is a Mobility Management Entity (MME), and the second network function is an Access and Mobility Management Function(AMF).

Specifically, Figure 4 illustrates a procedure where a UE is being served by a source

30 MME, but requires to register with a target AMF. More specifically, Figure 4 illustrates a procedure where the registration is based on location update, including a tracking area update (TAU).

In step 401, the UE sends to the Radio Access Network a Registration Request. This

35 contains information indicating that the Registration type is mobility registration, and a Temporary User ID for the UE indicating an identity of the source MME. The

Registration Request may optionally also contain parameters that the MME can parse. Such parameters can for example include the EPS UE Core Network Capability, the EPS key set identifier, and/or the EPC Non Access Stratum (NAS) sequence number. The Registration Request may optionally also contain parameters that the MME cannot
5 parse. Such parameters can for example include the UE 5G Core Network (5GCN) Capability, and/or a 5G parameter to support network slice selection (for example NSSAI).

The UE integrity protects at least a part of the Registration Request. In this example,
10 the UE integrity protects the whole Registration Request message. More specifically, in this example, the UE integrity protects the Registration Request message with a Message Authentication Code (MAC). The MAC may be computed with at least a part of the Extended Packet System (EPS) security context matching the one that is stored in the source MME. For example, the security context may contain keys to be used for
15 encryption and for integrity protection, but in some examples only the keys for integrity protection are used in computing the MAC.

The integrity protection making use of the legacy Non Access Stratum (NAS) security header enables the MME to verify the MAC, as described further below.

20

Thus, in step 401, the UE sends to the Radio Access Network the Registration Request, and the MAC included in the Registration Request.

In step 402, the RAN forwards the received Registration Request, also including the
25 MAC, to the target AMF.

In step 403, the target AMF sends a message to the source MME to request user information relating to the UE. In some examples, the message requesting UE information is a Context Request message. In some examples, the Context Request
30 message includes the complete integrity protected Registration Request message.

In step 404, the source MME receives the Context Request message, and checks the integrity of the integrity protected part of the received message. For example, in the cases described above, the source MME computes a MAC for the complete integrity
35 protected Registration Request message. The MAC is computed with the same part of the Extended Packet System (EPS) security context that is used by the UE. Thus, a

legacy MME is able to check the integrity of the included Registration Request message using the included legacy NAS security header.

Thus, the legacy MME is able to verify the entire registration request message which is
5 of 5G NAS type.

If the source MME determines that the message has not been tampered with, it sends the requested user information to the target AMF in response to the Context Request message.

10

If the source MME determines that the integrity check is failed, and hence that the message has potentially been tampered with, it may still send the requested user information to the target AMF, but it will indicate that the UE could not be authenticated. The failed authentication can be used by the target system as a trigger to authenticate
15 the UE in order to establish new security keys (since the user could not be authenticated using the existing security keys).

20

Figure 5 is a signalling diagram illustrating a fourth procedure in the example where the first network function is a Mobility Management Entity (MME), and the second network function is an Access and Mobility Management Function(AMF).

Specifically, Figure 5 illustrates a procedure where a UE is being served by a source MME, but requires to register with a target AMF. More specifically, Figure 5 illustrates a procedure where the registration is based on attach.

25

In step 501, the UE sends to the Radio Access Network a Registration Request. This contains information indicating that the Registration type is an initial registration, and a Temporary User ID for the UE indicating an identity of the source MME. The Registration Request may optionally also contain parameters that the MME can parse.
30 Such parameters can for example include the EPS UE Core Network Capability, the EPS key set identifier, and/or the EPC Non Access Stratum (NAS) sequence number. The Registration Request may optionally also contain parameters that the MME cannot parse. Such parameters can for example include the UE 5G Core Network (5GCN) Capability, and/or a 5G parameter to support network slice selection (for example
35 NSSAI).

The UE integrity protects at least a part of the Registration Request. In this example, the UE integrity protects the whole Registration Request message. More specifically, in this example, the UE integrity protects the Registration Request message with a Message Authentication Code (MAC). The MAC may be computed with at least a part
5 of the Extended Packet System (EPS) security context matching the one that is stored in the source MME. For example, the security context may contain keys to be used for encryption and for integrity protection, but in some examples only the keys for integrity protection are used in computing the MAC.

10 The integrity protection making use of the legacy Non Access Stratum (NAS) security header enables the MME to verify the MAC, as described further below.

Thus, in step 501, the UE sends to the Radio Access Network the Registration Request, and the MAC.

15

In step 502, the RAN forwards the received Registration Request, also including the MAC, to the target AMF.

In step 503, the target AMF sends a message to the source MME to request user
20 information relating to the UE. In some examples, the message requesting UE information is an Identification Request message. In some examples, the Identification Request message includes the complete integrity protected Registration Request message.

25 In step 504, the source MME receives the Identification Request message, and checks the integrity of the integrity protected part of the received message. For example, in the cases described above, the source MME computes a MAC for the complete integrity protected Registration Request message. The MAC is computed with the same part of the Extended Packet System (EPS) security context that is used by the
30 UE. Thus, a legacy MME is able to check the integrity of the included Registration Request message using the included legacy NAS security header.

Thus, the legacy MME is able to verify the entire registration request message which is of 5G NAS type.

35

If the source MME determines that the message has not been tampered with, it sends the requested user information to the target AMF in response to the Identification Request message.

- 5 If the source MME determines that the integrity check is failed, and hence that the message has potentially been tampered with, it will indicate that the UE could not be authenticated, and it may not send any security related information to the target AMF. The failed authentication can be used by the target system as a trigger to authenticate the UE in order to establish new security keys (since the user could not be
10 authenticated using the existing security keys).

Figure 6 is a block diagram illustrating an apparatus which may carry out methods for operating a user equipment device. The apparatus may be located in the user equipment device or may be located remotely therefrom.

15

As mentioned above, the term user equipment device (UE) is used herein to refer to any terminal device, whether that device is intended to be a user-operated device such as a smartphone, tablet or laptop computer, or the like, or whether that device is intended to operate independently, for example as a remote sensor of the like.

- 20 Similarly, the UE may be intended to operate from a generally fixed location, for example in the case of a closed-circuit TV camera or the like, or may be intended to be mobile, for example in the case of a smartphone, tablet or laptop computer, tracking device, or the like.

- 25 The apparatus 600 shown in Figure 6 comprises at least one transceiver 602 for connecting to various functions in a communications network, at least one processor 604 and at least one memory 606. The memory 606 contains instructions executable by the processor 604 such that the apparatus 600 is operative to conduct some or all of the steps of the method for operating a UE described above and set out in the claims.

30

Figure 7 illustrates an alternative example apparatus 700, which may implement methods for operating a UE as discussed above and set out in the claims, for example on receipt of suitable instructions from a computer program. It will be appreciated that the modules illustrated in Figure 7 may be realised in any appropriate combination of
35 hardware and/or software. For example, the modules may comprise one or more

processors and one or more memories containing instructions executable by the one or more processors. The modules may be integrated to any degree.

Referring to Figure 7, the apparatus 700 comprises, for when the UE is served by a source first network function in a first network and requires to register with a target second network function in a second network: a generating module 702, for generating a registration request with integrity protection for at least a part of the registration request; and a sending module 704, for sending an integrity protected part of the registration request to the source first network function via the target second network function.

Figure 8 illustrates a first example of an apparatus 800 which may carry out methods for operating a first network function, which may in this illustrated example be a Mobility Management Entity (MME) function. The apparatus may for example comprise a network node and may comprise a plurality of network nodes. The apparatus may be located in a first network node or may be located remotely therefrom.

The apparatus 800 may carry out the methods for example on receipt of suitable instructions from a computer program. Referring to Figure 8, the apparatus comprises interfaces 802, for connecting to other functions and terminals in the network, a processor 804, and a memory 806. The memory 806 contains instructions executable by the processor 804 such that the apparatus 800 is operative to conduct some or all of the steps of the methods for operating a first network function described above and set out in the claims.

Figure 9 illustrates an alternative example apparatus 900, which may implement methods for operating a first network function, which may in this illustrated example be a Mobility Management Entity (MME) function as discussed above and set out in the claims, for example on receipt of suitable instructions from a computer program. The apparatus may for example comprise a network node and may comprise a plurality of network nodes. It will be appreciated that the modules illustrated in Figure 9 may be realised in any appropriate combination of hardware and/or software. For example, the modules may comprise one or more processors and one or more memories containing instructions executable by the one or more processors. The modules may be integrated to any degree.

Referring to Figure 9, the apparatus 900 comprises a receiving module 902 for receiving at least a part of a registration request from a User Equipment (UE) via a target second network function in a second wireless communications network, wherein the source first network function is serving the UE, and wherein the received
5 registration request requests registration with said target second network function, and a checking module 904 for checking integrity of the received at least part of a registration request.

Figure 10 illustrates a first example of an apparatus 1000 which may carry out methods
10 for operating a second network function, which may in this illustrated example be an Access and Mobility Management Function(AMF) function. The apparatus may for example comprise a network node and may comprise a plurality of network nodes. The apparatus may be located in a second network node or may be located remotely therefrom.

15 The apparatus 1000 may carry out the methods for example on receipt of suitable instructions from a computer program. Referring to Figure 10, the apparatus comprises interfaces 1002, for connecting to other functions and terminals in the network, a processor 1004, and a memory 1006. The memory 1006 contains
20 instructions executable by the processor 1004 such that the apparatus 1000 is operative to conduct some or all of the steps of the methods for operating a second network function described above and set out in the claims.

Figure 11 illustrates an alternative example apparatus 1100, which may implement
25 methods for operating a second network function, which may in this illustrated example be an Access and Mobility Management Function(AMF) function as discussed above and set out in the claims, for example on receipt of suitable instructions from a computer program. The apparatus may for example comprise a network node and may comprise a plurality of network nodes. It will be appreciated that the modules
30 illustrated in Figure 11 may be realised in any appropriate combination of hardware and/or software. For example, the modules may comprise one or more processors and one or more memories containing instructions executable by the one or more processors. The modules may be integrated to any degree.

35 Referring to Figure 11, the apparatus 1100 comprises a receiving module 1102 for receiving a registration request from a User Equipment (UE); and a forwarding module

1104 for forwarding a request to retrieve information about the UE to a first network function in a first network serving the UE.

Figure 12 is a flow chart, illustrating a procedure performed in a User Equipment (UE), wherein the UE is served by a source first network function in a first network and requires to register with a target second network function in a second network. In step 1200, the UE generates a registration request with integrity protection for at least a part of the registration request. In step 1202, the UE sends an integrity protected part of the registration request to the source first network function via the target second network function.

Figure 13 is a flow chart, illustrating a procedure performed in a source first network function in a first wireless communications network. In step 1300, the first network function receives at least a part of a registration request from a User Equipment (UE) via a target second network function in a second wireless communications network, wherein the source first network function is serving the UE, and wherein the received registration request requests registration with said target second network function. In step 1302, the first network function checks the integrity of the received at least part of a registration request.

20

Figure 14 is a flow chart, illustrating a procedure performed in a second network function in a second network. In step 1400, the second network function receives a registration request from a User Equipment (UE). In step 1402, the second network function forwards a request to retrieve information about the UE to a first network function in a first network serving the UE.

25

According to aspects of the present disclosure, there is provided a carrier containing a computer program for performing any of the methods as discussed above, wherein the carrier comprises one of an electronic signal, optical signal, radio signal or computer readable storage medium.

30

According to aspects of the present disclosure, there is provided a computer program product comprising non transitory computer readable media having stored thereon a computer program as discussed above.

35

There is thus described methods and network elements that provide a mechanism for the protection of the registration request and hence mitigate against threats on the air interface such as man in the middle or replay attacks, and that provide a mechanism for a source network function such as an MME to authenticate a UE on behalf of a
5 target network function such as an AMF.

The following are certain enumerated embodiments further illustrating various aspects the disclosed subject matter.

- 10 1. A method for operating a User Equipment (UE),
wherein the UE is served by a source first network node in a first network and requires to register with a target second network node in a second network,
the method comprising:
generating a registration request with integrity protection for at least a part of the
15 registration request; and
sending the integrity protected part of the registration request to the source first network node via the target second network node.
2. A method according to item 1, wherein the first network node is a Mobility
20 Management Entity (MME) node.
3. A method according to item 1 or 2, wherein the second network node is an Access and Mobility Management Function(AMF) node.
- 25 4. A method according to item 1, 2 or 3, wherein the step of generating a registration request with integrity protection comprises generating a Message Authentication Code (MAC).
5. A method according to item 4, wherein the step of generating the registration
30 request with integrity protection comprises generating a Message Authentication Code (MAC) using information shared between the UE and the source first network node.
6. A method according to item 5, wherein the first network node is a Mobility Management Entity (MME) node, and the information that is shared between the UE
35 and the source MME is at least a part of an Evolved Packet System (EPS) security context.

7. A method according to one of items 1-6, wherein the first network node is a Mobility Management Entity (MME) node, and the integrity protected part of the registration request is an Evolved Packet Core (EPC) Non-Access Stratum (NAS) message.
8. A method according to item 7, wherein the EPC NAS message is a Tracking Area Update (TAU) request.
9. A method according to item 8, wherein the TAU request can be parsed by the source MME.
10. A method according to item 7, wherein the EPC NAS message is an Attach request.
11. A method according to item 10, wherein the Attach request can be parsed by the source MME.
12. A method according to one of items 1-6, wherein the second network node is an Access and Mobility Management Function (AMF) node, and the registration request is a 5G Non-Access Stratum (NAS) message.
13. A method according to item 12, wherein the integrity protected at least part of the registration request is the whole registration request.
14. A method according to item 12 or 13, wherein the registration request is a mobility registration request.
15. A method according to item 12 or 13, wherein the registration request is an attach registration request.
16. A User Equipment (UE), comprising a processor and a memory, the memory containing instructions for causing the processor to perform a method comprising, when the UE is served by a source first network node in a first network and requires to register with a target second network node in a second network:

generating a registration request with integrity protection for at least a part of the registration request; and

sending the integrity protected part of the registration request to the source first network node via the target second network node.

5

17. A UE according to item 16, wherein the first network node is a Mobility Management Entity (MME) node.

18. A UE according to item 16 or 17, wherein the second network node is an Access and Mobility Management Function (AMF) node.

10

19. A UE according to item 16, 17 or 18, wherein the step of generating a registration request with integrity protection comprises generating a Message Authentication Code (MAC).

15

20. A UE according to item 19, wherein the step of generating the registration request with integrity protection comprises generating a Message Authentication Code (MAC) using information shared between the UE and the source first network node.

21. A UE according to item 20, wherein the first network node is a Mobility Management Entity (MME) node, and the information that is shared between the UE and the source MME is at least a part of an Evolved Packet System (EPS) security context.

20

22. A UE according to one of items 16-21, wherein the first network node is a Mobility Management Entity (MME) node, and the integrity protected part of the registration request is an Evolved Packet Core (EPC) Non-Access Stratum (NAS) message.

25

23. A UE according to item 22, wherein the EPC NAS message is a Tracking Area Update (TAU) request.

30

24. A UE according to item 23, wherein the TAU request can be parsed by the source MME.

25. A UE according to item 22, wherein the EPC NAS message is an Attach request.

35

26. A UE according to item 25, wherein the Attach request can be parsed by the source MME.
27. A UE according to one of items 16-21, wherein the second network node is an
5 Access and Mobility Management Function(AMF) node, and the registration request is a 5G Non-Access Stratum (NAS) message.
28. A UE according to item 27, wherein the integrity protected at least part of the registration request is the whole registration request.
- 10 29. A UE according to item 27 or 28, wherein the registration request is a mobility registration request.
30. A UE according to item 27 or 28, wherein the registration request is an attach
15 registration request.
31. A User Equipment (UE), the UE being configured to perform a method in accordance with any one of items 1-15.
- 20 32. A User Equipment (UE), comprising, for when the UE is served by a source first network node in a first network and requires to register with a target second network node in a second network:
- a generating module, for generating a registration request with integrity protection for at least a part of the registration request; and
- 25 style="padding-left: 40px;">a sending module, for sending the integrity protected part of the registration request to the source first network node via the target second network node.
33. A computer program product, containing instructions for causing a User Equipment to perform a method in accordance with any one of items 1-15.
- 30 34. A method for operating a source first network node in a first wireless communications network, the method comprising:
- receiving at least a part of a registration request from a User Equipment (UE) via a target second network node in a second wireless communications network,
- 35 style="padding-left: 40px;">wherein the source first network node is serving the UE, and

wherein the received registration request requests registration with said target second network node,

the method comprising:

checking integrity of the received at least part of a registration request.

5

35. A method according to item 34, wherein the first network node is a Mobility Management Entity (MME) node.

10 36. A method according to item 34 or 35, wherein the second network node is an Access and Mobility Management Function (AMF) node.

37. A method according to item 34, 35 or 36, wherein the step of checking the integrity comprises generating a Message Authentication Code (MAC).

15 38. A method according to item 37, wherein the step of checking the integrity comprises generating the Message Authentication Code (MAC) using information shared between the UE and the source first network node.

20 39. A method according to item 38, wherein the first network node is a Mobility Management Entity (MME) node, and the information that is shared between the UE and the source MME is at least part of an Evolved Packet System (EPS) security context.

25 40. A method according to one of items 34-39, wherein the first network node is a Mobility Management Entity (MME) node, and the integrity protected part of the registration request is an Evolved Packet Core (EPC) Non-Access Stratum (NAS) message.

30 41. A method according to item 40, wherein the EPC NAS message is a Tracking Area Update (TAU) request.

42. A method according to item 41, wherein the TAU request can be parsed by the source MME.

35 43. A method according to item 40, wherein the EPC NAS message is an Attach request.

44. A method according to item 43, wherein the Attach request can be parsed by the source MME.

45. A method according to one of items 34-39, wherein the second network node is
5 an Access and Mobility Management Function(AMF) node, and the registration request is a 5G Non-Access Stratum (NAS) message.

46. A method according to item 45, wherein the integrity protected at least part of the registration request is the whole registration request.

10

47. A method according to item 45 or 46, wherein the registration request is a mobility registration request.

48. A method according to item 45 or 46, wherein the registration request is an
15 attach registration request.

49. A method according to one of items 34-48, the method further comprising:
in response to the received at least part of a registration request passing the integrity check, providing user information to the target second network node.

20

50. A method according to one of items 34-48, the method further comprising:
in response to the received at least part of a registration request failing the integrity check, notifying the second network node that the UE may not be authenticated.

25

51. A first network node for use in a first wireless communications network, the first network node comprising a processor and a memory, the memory containing instructions for causing the processor to perform a method comprising:
receiving at least a part of a registration request from a User Equipment (UE) via
30 a target second network node in a second wireless communications network,
wherein the source first network node is serving the UE, and
wherein the received registration request requests registration with said target second network node,

the method comprising:
35 checking integrity of the received at least part of a registration request.

52. A first network node according to item 51, wherein the first network node is a Mobility Management Entity (MME) node.
53. A first network node according to item 51 or 52, wherein the second network
5 node is an Access and Mobility Management Function (AMF) node.
54. A first network node according to item 51, 52 or 53, wherein the step of checking the integrity comprises generating a Message Authentication Code (MAC).
- 10 55. A first network node according to item 54, wherein the step of checking the integrity comprises generating the Message Authentication Code (MAC) using information shared between the UE and the source first network node.
56. A first network node according to item 55, wherein the first network node is a
15 Mobility Management Entity (MME) node, and the information that is shared between the UE and the source MME is at least part of an Evolved Packet System (EPS) security context.
57. A first network node according to one of items 51-56, wherein the first network
20 node is a Mobility Management Entity (MME) node, and the integrity protected part of the registration request is an Evolved Packet Core (EPC) Non-Access Stratum (NAS) message.
58. A first network node according to item 57, wherein the EPC NAS message is a
25 Tracking Area Update (TAU) request.
59. A first network node according to item 58, wherein the TAU request can be parsed by the source MME.
- 30 60. A first network node according to item 57, wherein the EPC NAS message is an Attach request.
61. A first network node according to item 60, wherein the Attach request can be parsed by the source MME.

62. A first network node according to one of items 51-56, wherein the second network node is an Access and Mobility Management Function(AMF) node, and the registration request is a 5G Non-Access Stratum (NAS) message.

5 63. A first network node according to item 62, wherein the integrity protected at least part of the registration request is the whole registration request.

64. A first network node according to item 62 or 63, wherein the registration request is a mobility registration request.

10

65. A first network node according to item 62 or 63, wherein the registration request is an attach registration request.

15

66. A first network node according to one of items 51-65, the method further comprising:

in response to the received at least part of a registration request passing the integrity check, providing user information to the target second network node.

20

67. A first network node according to one of items 51-65, the method further comprising:

in response to the received at least part of a registration request failing the integrity check, notifying the second network node that the UE may not be authenticated.

25

68. A first network node, the first network node being configured to perform a method in accordance with any one of items 34-50.

69. A first network node for use in a first wireless communications network, the network node comprising:

30

a receiving module for receiving at least a part of a registration request from a User Equipment (UE) via a target second network node in a second wireless communications network,

wherein the source first network node is serving the UE, and

wherein the received registration request requests registration with said target

35

second network node,

and

a checking module for checking integrity of the received at least part of a registration request.

70. A computer program product, containing instructions for causing a first network
5 node to perform a method in accordance with any one of items 34-50.

71. A method for operating a second network node in a second network, the method
10 comprising:
receiving a registration request from a User Equipment (UE); and
forwarding a request to retrieve information about the UE to a first network node
in a first network serving the UE.

15 72. A method according to item 71, wherein the second network node is an Access
and Mobility Management Function(AMF) node.

73. A method according to item 71 or 72, wherein the first network node is a Mobility
Management Entity (MME) node.
20

74. A method according to item 71, 72 or 73, comprising receiving the registration
request from the User Equipment (UE) via an access network.

75. A method according to item 71, 72, 73 or 74, wherein the request to retrieve
25 information about the UE comprises a context request.

76. A method according to item 75, wherein the first network node is a Mobility
Management Entity (MME) node, and the context request comprises a Tracking Area
Update Request from the registration request.
30

77. A method according to item 75, wherein the first network node is a Mobility
Management Entity (MME) node, and the context request comprises the whole
registration request.

35 78. A method according to item 71, 72, 73 or 74, wherein the request to retrieve
information about the UE comprises an identification request.

79. A method according to item 78, wherein the first network node is a Mobility Management Entity (MME) node, and the identification request comprises an Attach Request from the registration request.

5

80. A method according to item 78, wherein the first network node is a Mobility Management Entity (MME) node, and the identification request comprises the whole registration request.

10 81. A method according to any one of items 71 to 80, wherein the request to retrieve information about the UE comprises at least a part of the registration request, and wherein said part of the registration request is integrity protected.

15 82. A second network node for use in a second wireless communications network, the second network node comprising a processor and a memory, the memory containing instructions for causing the processor to perform a method comprising:
receiving a registration request from a User Equipment (UE); and
forwarding a request to retrieve information about the UE to a first network node in a first network serving the UE.

20

83. A second network node according to item 82, wherein the second network node is an Access and Mobility Management Function(AMF) node.

25 84. A second network node according to item 82 or 83, wherein the first network node is a Mobility Management Entity (MME) node.

85. A second network node according to item 82, 83 or 84, wherein the method comprises receiving the registration request from the User Equipment (UE) via an access network.

30

86. A second network node according to item 82, 83, 84 or 85, wherein the request to retrieve information about the UE comprises a context request.

35 87. A second network node according to item 86, wherein the first network node is a Mobility Management Entity (MME) node, and the context request comprises a Tracking Area Update Request from the registration request.

88. A second network node according to item 86, wherein the first network node is a Mobility Management Entity (MME) node, and the context request comprises the whole registration request.

5

89. A second network node according to item 82, 83, 84 or 85, wherein the request to retrieve information about the UE comprises an identification request.

90. A second network node according to item 89, wherein the first network node is a Mobility Management Entity (MME) node, and the identification request comprises an Attach Request from the registration request.

91. A second network node according to item 89, wherein the first network node is a Mobility Management Entity (MME) node, and the identification request comprises the whole registration request.

92. A second network node according to any one of items 82 to 91, wherein the request to retrieve information about the UE comprises at least a part of the registration request, and wherein said part of the registration request is integrity protected.

20

93. A second network node for use in a second wireless communications network, the second network node, the second network node being configured for performing a method in accordance with any of items 71-81.

94. A second network node for use in a second wireless communications network, the second network node comprising:
a receiving module for receiving a registration request from a User Equipment (UE); and
a forwarding module for forwarding a request to retrieve information about the UE to a first network node in a first network serving the UE.

30

95. A computer program product, containing instructions for causing a second network node to perform a method in accordance with any one of items 71-81.

35

It should be noted that the above-mentioned embodiments illustrate rather than limit the invention, and that those skilled in the art will be able to design many alternative embodiments without departing from the scope of the appended claims. The word “comprising” does not exclude the presence of elements or steps other than those
5 listed in a claim, “a” or “an” does not exclude a plurality, and a single feature or other unit may fulfil the functions of several units recited in the claims. Any reference signs in the claims shall not be construed so as to limit their scope.

CLAIMS

1. A method for operating a User Equipment (UE),
5 wherein the UE is served by a source first network function in a first network and requires to register with a target second network function in a second network,
the method comprising:
generating a registration request with integrity protection for at least a part of the registration request; and
10 sending an integrity protected part of the registration request to the source first network function via the target second network function.
2. A method according to claim 1, wherein the first network function is a Mobility Management Entity (MME) function.
15
3. A method according to claim 1 or 2, wherein the second network function is an Access and Mobility Management Function (AMF) function.
4. A method according to claim 1, 2 or 3, wherein the step of generating a
20 registration request with integrity protection comprises generating a Message Authentication Code (MAC).
5. A method according to claim 4, wherein the step of generating the registration request with integrity protection comprises generating a Message Authentication Code
25 (MAC) using information shared between the UE and the source first network function.
6. A method according to claim 5, wherein the first network function is a Mobility Management Entity (MME) function, and the information that is shared between the UE and the source MME is at least a part of an Evolved Packet System (EPS) security
30 context.
7. A method according to one of claims 1-6, wherein the first network function is a Mobility Management Entity (MME) function, and an integrity protected part of the registration request is an Evolved Packet Core (EPC) Non-Access Stratum (NAS)
35 message.

8. A method according to claim 7, when dependent upon claims 5 or 6, wherein the EPS NAS message is integrity protected with the MAC generated using information shared between the UE and the source first network function.
- 5 9. A method according to claim 7 or 8, wherein the EPC NAS message is a Tracking Area Update (TAU) request or an Attach request.
- 10 10. A method according to claim 9, wherein the TAU request can be parsed by the source MME.
11. A method according to claim 9, wherein the Attach request can be parsed by the source MME.
12. A method according to one of the preceding claims, wherein the second network
15 function is an Access and Mobility Management Function (AMF) function, and the registration request is a 5G Non-Access Stratum (NAS) message.
13. A method according to claim 12, when dependent on any one of claims 4 to 11,
20 wherein the step of generating the registration request with integrity protection comprises generating a Message Authentication Code (MAC) using information shared between the UE and a network function in the second network.
14. A method according to claim 13, wherein the information that is shared between
25 the UE and a network function in the second network is at least a part of a 5G security context.
15. A method according to any one of claims 12 to 14, wherein an integrity protected at least part of the registration request is the whole registration request.
- 30 16. A method according to claim 15, when dependent on claims 13 or 14, wherein the whole registration request is integrity protected with the MAC generated using information shared between the UE and a network function in the second network.
- 35 17. A method according to any one of claims 12 to 16, wherein the registration request is a mobility registration request or an initial registration request.

18. A method according to any one of claims 12 to 17, further comprising:
 retrieving an EPS security context used for communication with the source first network function;
 deriving a mapped 5G security context from the retrieved EPS security context;
 5 generating a Key Set Identifier, KSI, to identify the retrieved EPS security context; and
 including the KSI in the registration request.
19. A User Equipment (UE), the UE being adapted to perform a method comprising,
 10 when the UE is served by a source first network function in a first network and requires to register with a target second network function in a second network:
 generating a registration request with integrity protection for at least a part of the registration request; and
 sending an integrity protected part of the registration request to the source first
 15 network function via the target second network function.
20. A User Equipment (UE), the UE being configured to perform a method in accordance with any one of claims 1-18.
- 20 21. A computer program product, containing instructions for causing a User Equipment to perform a method in accordance with any one of claims 1-18.
22. A method for operating a source first network function in a first wireless communications network, the method comprising:
 25 receiving at least a part of a registration request from a User Equipment (UE) via a target second network function in a second wireless communications network,
 wherein the source first network function is serving the UE, and
 wherein the received registration request requests registration with said target second network function,
 30 the method comprising:
 checking integrity of the received at least part of a registration request.
23. A method according to claim 22, wherein the first network function is a Mobility Management Entity (MME) function.

24. A method according to claim 22 or 23, wherein the second network function is an Access and Mobility Management Function(AMF) function.

25. A method according to claim 22, 23 or 24, wherein the step of checking the integrity comprises generating a Message Authentication Code (MAC).

26. A method according to claim 25, wherein the step of checking the integrity comprises generating the Message Authentication Code (MAC) using information shared between the UE and the source first network function.

27. A method according to claim 26, wherein the first network function is a Mobility Management Entity (MME) function, and the information that is shared between the UE and the source MME is at least part of an Evolved Packet System (EPS) security context.

28. A method according to one of claims 22-27, wherein the first network function is a Mobility Management Entity (MME) function, and the integrity protected part of the registration request is an Evolved Packet Core (EPC) Non-Access Stratum (NAS) message.

29. A method according to claim 28, wherein the EPC NAS message is a Tracking Area Update (TAU) request or an attach request.

30. A method according to claim 29, wherein the TAU request can be parsed by the source MME.

31. A method according to claim 29, wherein the Attach request can be parsed by the source MME.

32. A method according to one of claims 22-27, wherein the second network function is an Access and Mobility Management Function(AMF) function, and the registration request is a 5G Non-Access Stratum (NAS) message.

33. A method according to claim 32, wherein the integrity protected at least part of the registration request is the whole registration request.

34. A method according to claim 32 or 33, wherein the registration request is a mobility registration request or an initial registration request.
35. A method according to one of claims 22-34, the method further comprising:
5 in response to the received at least part of a registration request passing the integrity check, providing user information to the target second network function.
36. A method according to one of claims 22-34, the method further comprising:
10 in response to the received at least part of a registration request failing the integrity check, notifying the second network function that the UE may not be authenticated.
37. Apparatus for implementing a first network function for use in a first wireless communications network, the apparatus being adapted to perform a method
15 comprising:
receiving at least a part of a registration request from a User Equipment (UE) via a target second network function in a second wireless communications network,
wherein the source first network function is serving the UE, and
wherein the received registration request requests registration with said target
20 second network function,
the method comprising:
checking integrity of the received at least part of a registration request.
38. Apparatus for implementing a first network function, the first network function
25 being configured to perform a method in accordance with any one of claims 22-36.
39. A computer program product, containing instructions for causing a first network function to perform a method in accordance with any one of claims 22-36.
- 30 40. A method for operating a second network function in a second network, the method comprising:
receiving a registration request from a User Equipment (UE); and
forwarding a request to retrieve information about the UE to a first network function in a first network serving the UE.

41. A method according to claim 40, wherein the second network function is an Access and Mobility Management Function(AMF) function.
42. A method according to claim 40 or 41, wherein the first network function is a
5 Mobility Management Entity (MME) function.
43. A method according to claim 40, 41 or 42, comprising receiving the registration request from the User Equipment (UE) via an access network.
- 10 44. A method according to claim 40, 41, 42 or 43, wherein the request to retrieve information about the UE comprises a context request.
45. A method according to claim 44, wherein the first network function is a Mobility Management Entity (MME) function, and the context request comprises a Tracking
15 Area Update Request from the registration request.
46. A method according to claim 44, wherein the first network function is a Mobility Management Entity (MME) function, and the context request comprises the whole registration request.
20
47. A method according to claim 40, 41, 42 or 43, wherein the request to retrieve information about the UE comprises an identification request.
48. A method according to claim 47, wherein the first network function is a Mobility
25 Management Entity (MME) function, and the identification request comprises an Attach Request from the registration request.
49. A method according to claim 47, wherein the first network function is a Mobility Management Entity (MME) function, and the identification request comprises the whole
30 registration request.
50. A method according to any one of claims 40 to 49, wherein the request to retrieve information about the UE comprises at least a part of the registration request, and wherein said part of the registration request is integrity protected.
35

51. A method according to claim on 50, wherein the second network function is an Access and Mobility Management Function(AMF) function and the first network function is a Mobility Management Entity (MME) function and wherein said part of the registration request is integrity protected using an EPS security context.

5

52. A method according to any one of claims 40 to 51, wherein the second network function is an Access and Mobility Management Function(AMF) function and the first network function is a Mobility Management Entity (MME) function and wherein the registration request is integrity protected using a 5G security context.

10

53. A method according to claim 52, further comprising checking the integrity of the received registration request.

54. A method according to claim 53, wherein the step of checking the integrity comprises generating a Message Authentication Code (MAC) using the 5G security context.

55. A method according to claim 53 or 54, further comprising:
in response to the received registration request passing the integrity check,
discarding a response received from the first network function to the request to retrieve information.

56. A method according to any one of claims 53 to 55, further comprising:
in response to the received registration request failing the integrity check,
performing at least one of:
deriving a mapped 5G security context from an EPS security context received from the first function in response to the request to retrieve information; or
initiating an authentication procedure to create a new 5G security context.

57. A method according to claim 52 further comprising:
determining that the 5G security context used to integrity protect the registration request is unavailable, and performing at least one of:
deriving a mapped 5G security context from an EPS security context received from the first function in response to the request to retrieve information; or
initiating an authentication procedure to create a new 5G security context.

58. A method according to any one of claims 40 to 51, wherein the second network function is an Access and Mobility Management Function(AMF) function and the first network function is a Mobility Management Entity (MME) function, and wherein the registration request includes a Key Set Identifier, KSI, the method further comprising:
- 5 using the KSI to identify an EPS security context from a response received from the first function to the request to retrieve information; and
- deriving a mapped 5G security context from the identified EPS security context.
59. Apparatus for implementing a second network function for use in a second
- 10 wireless communications network, the apparatus being adapted to perform a method comprising:
- receiving a registration request from a User Equipment (UE); and
- forwarding a request to retrieve information about the UE to a first network function in a first network serving the UE.
- 15 60. Apparatus for implementing a second network function for use in a second wireless communications network, the apparatus being configured for performing a method in accordance with any of claims 40-58.
- 20 61. A computer program product, containing instructions for causing a second network function to perform a method in accordance with any one of claims 40-58.

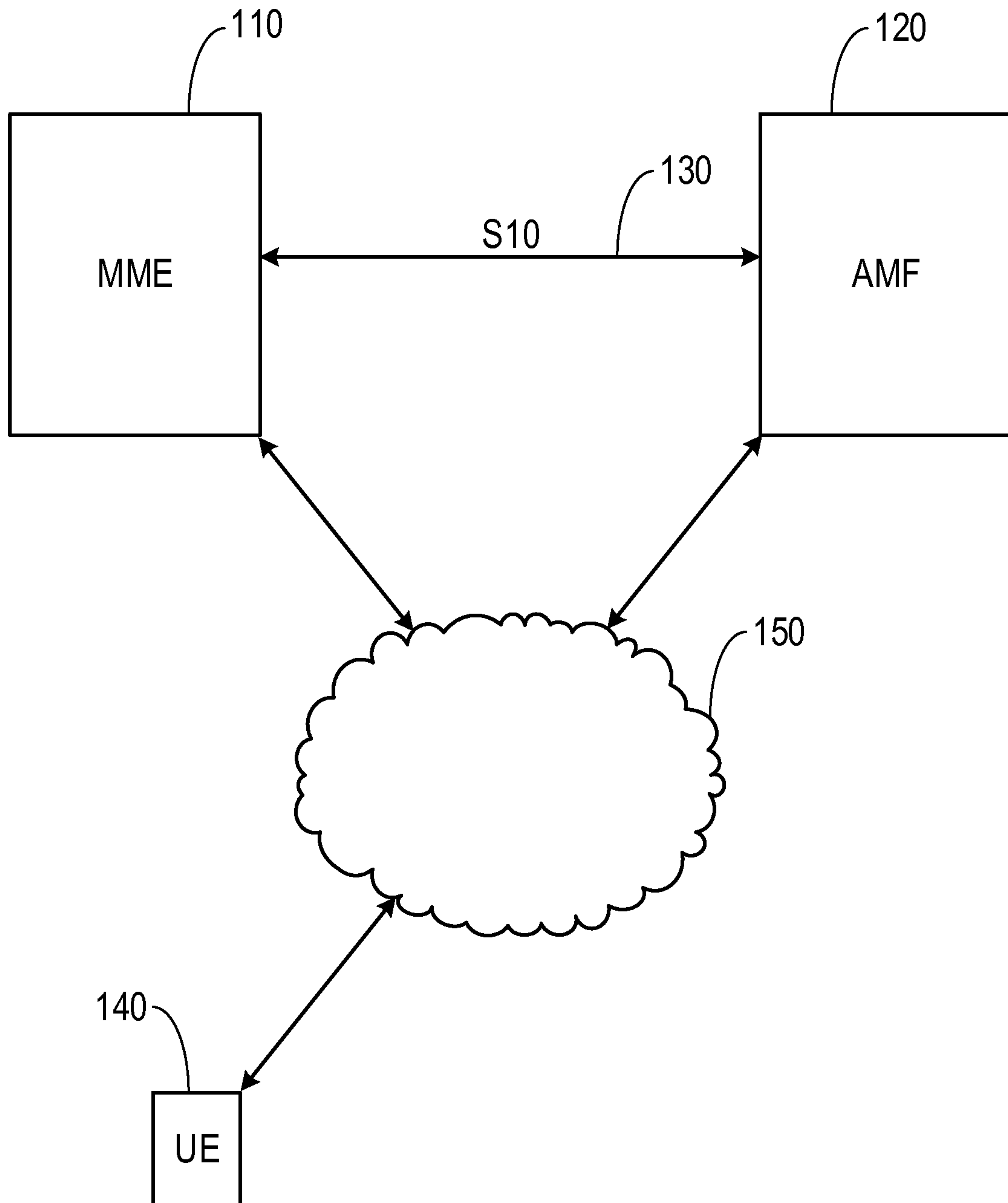


Figure 1

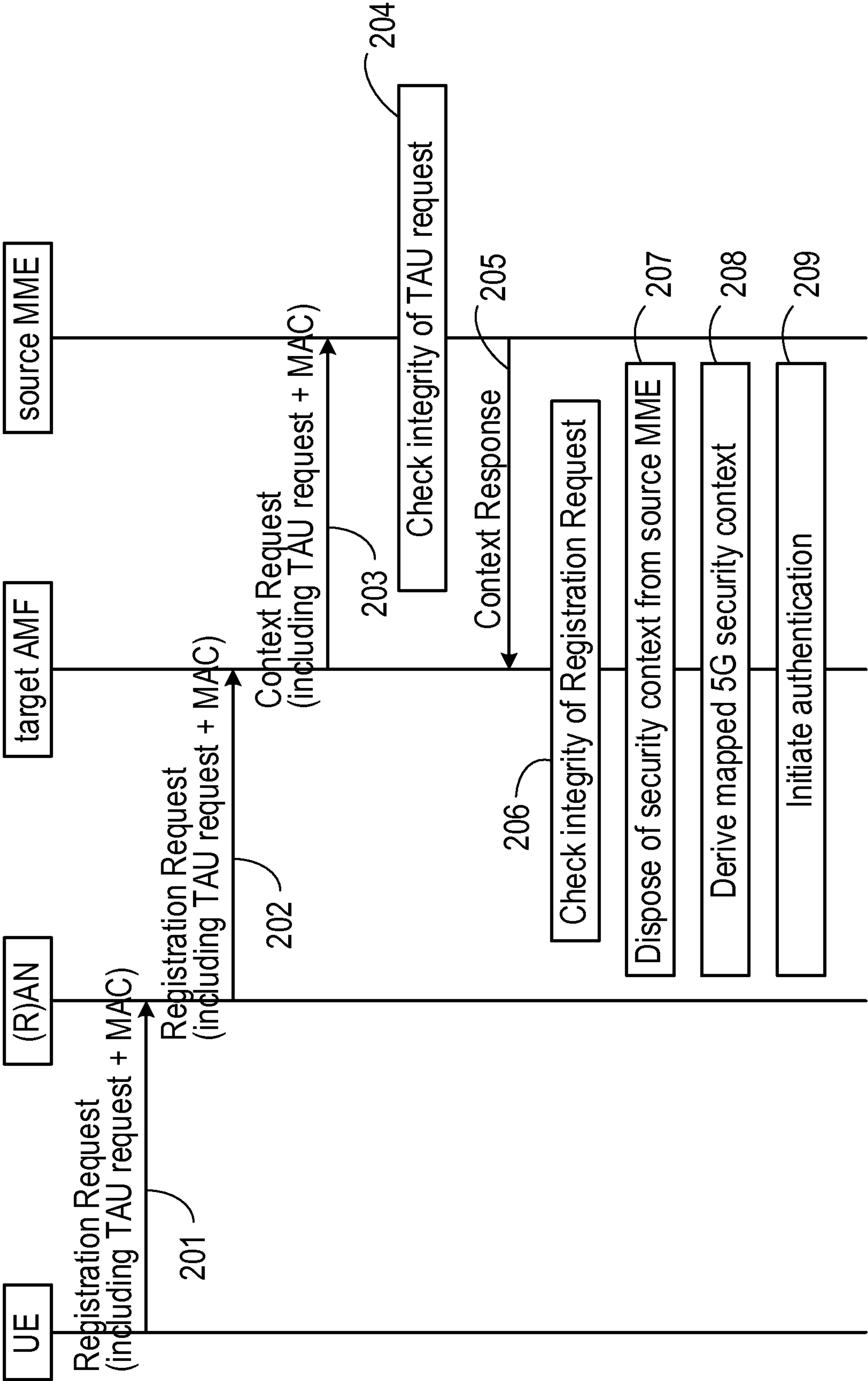


Figure 2

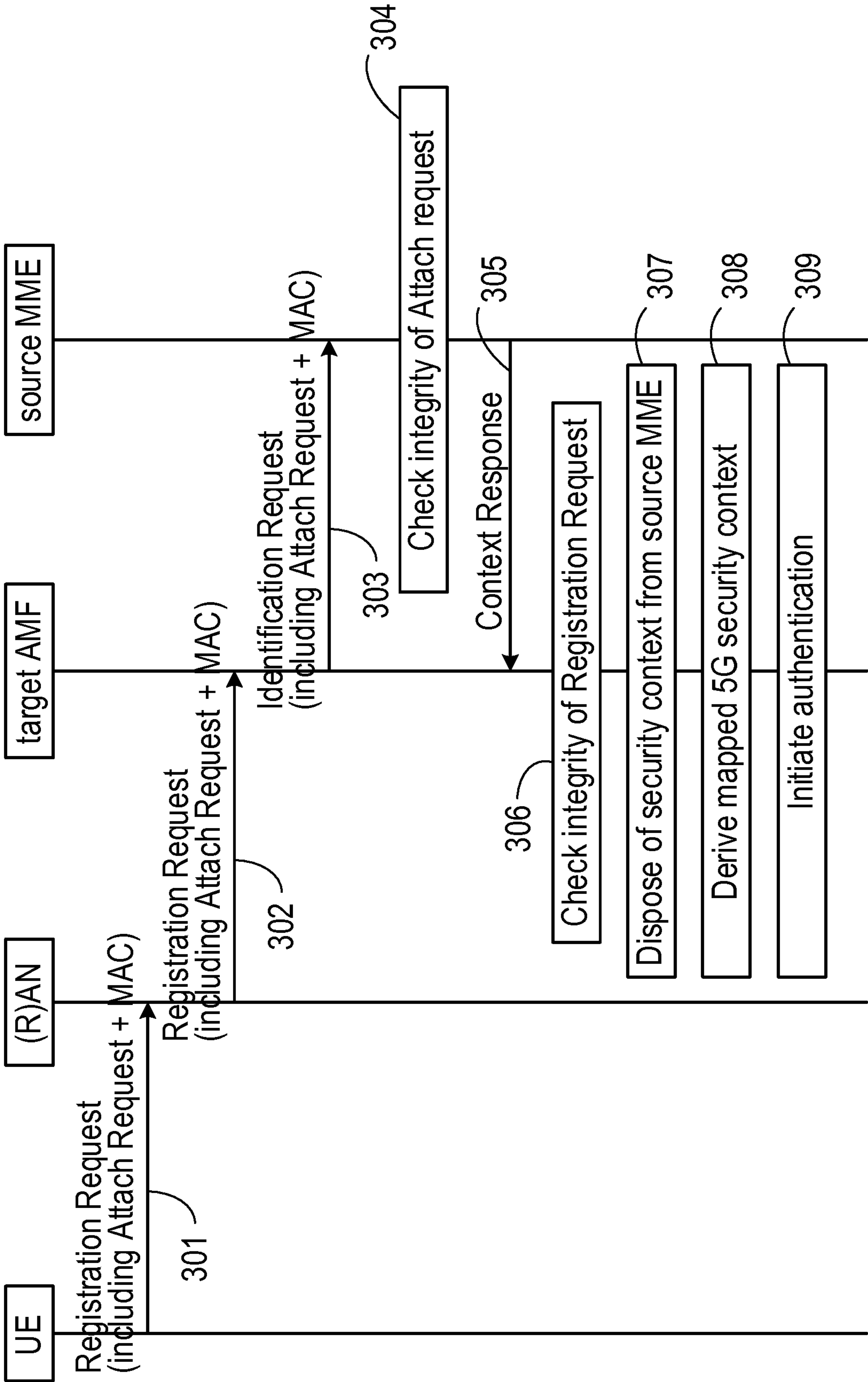


Figure 3

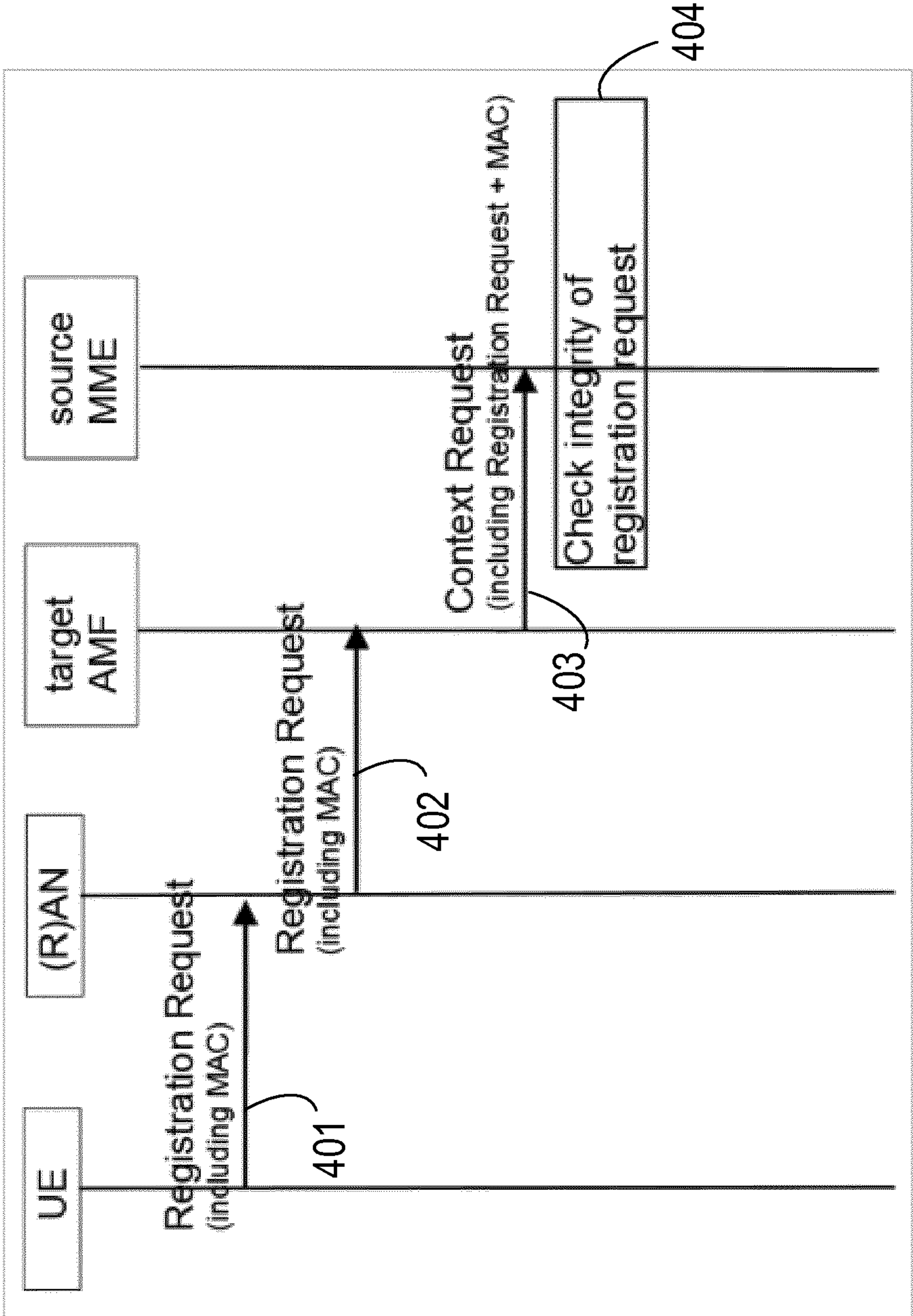


Figure 4

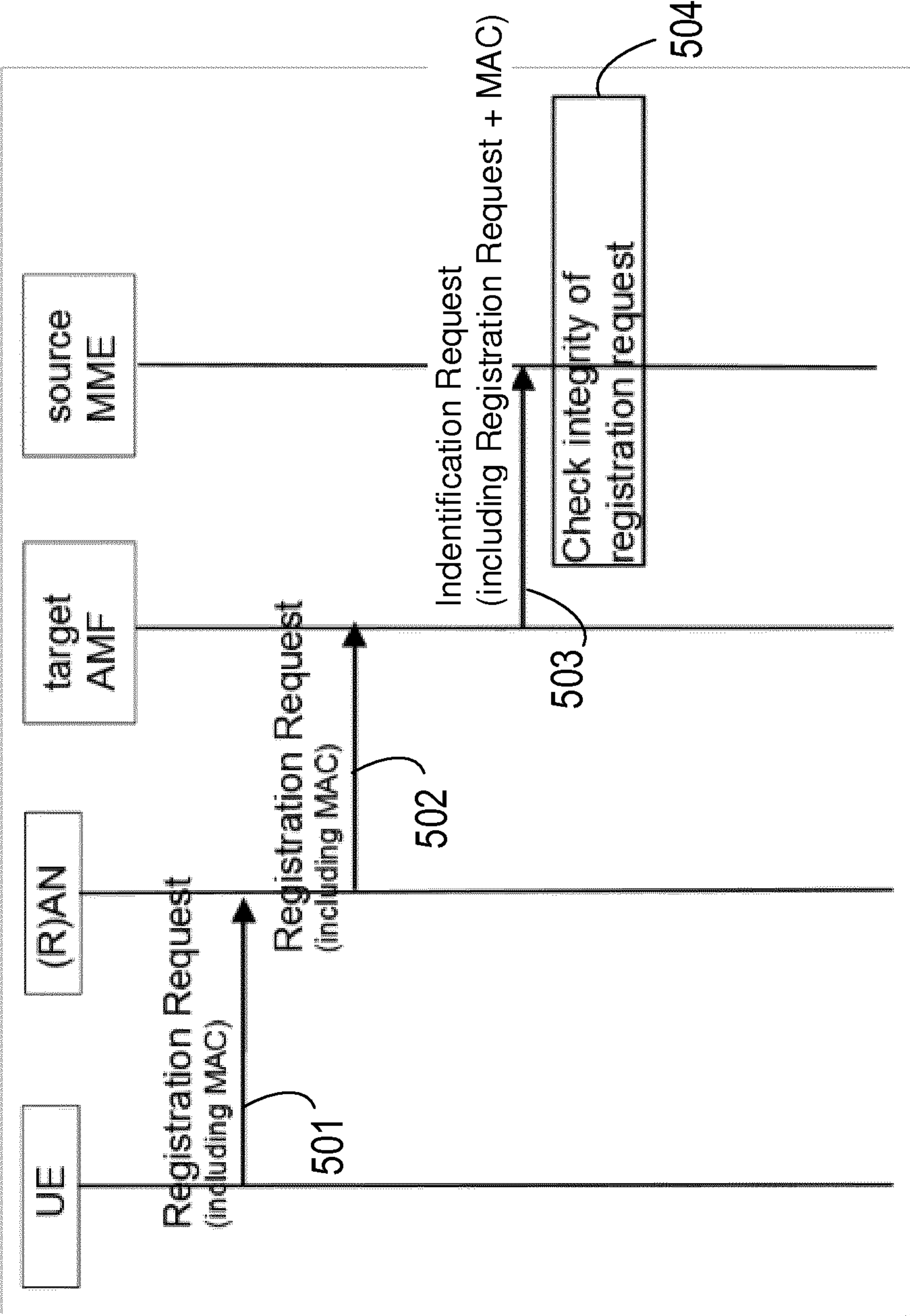


Figure 5

6/8

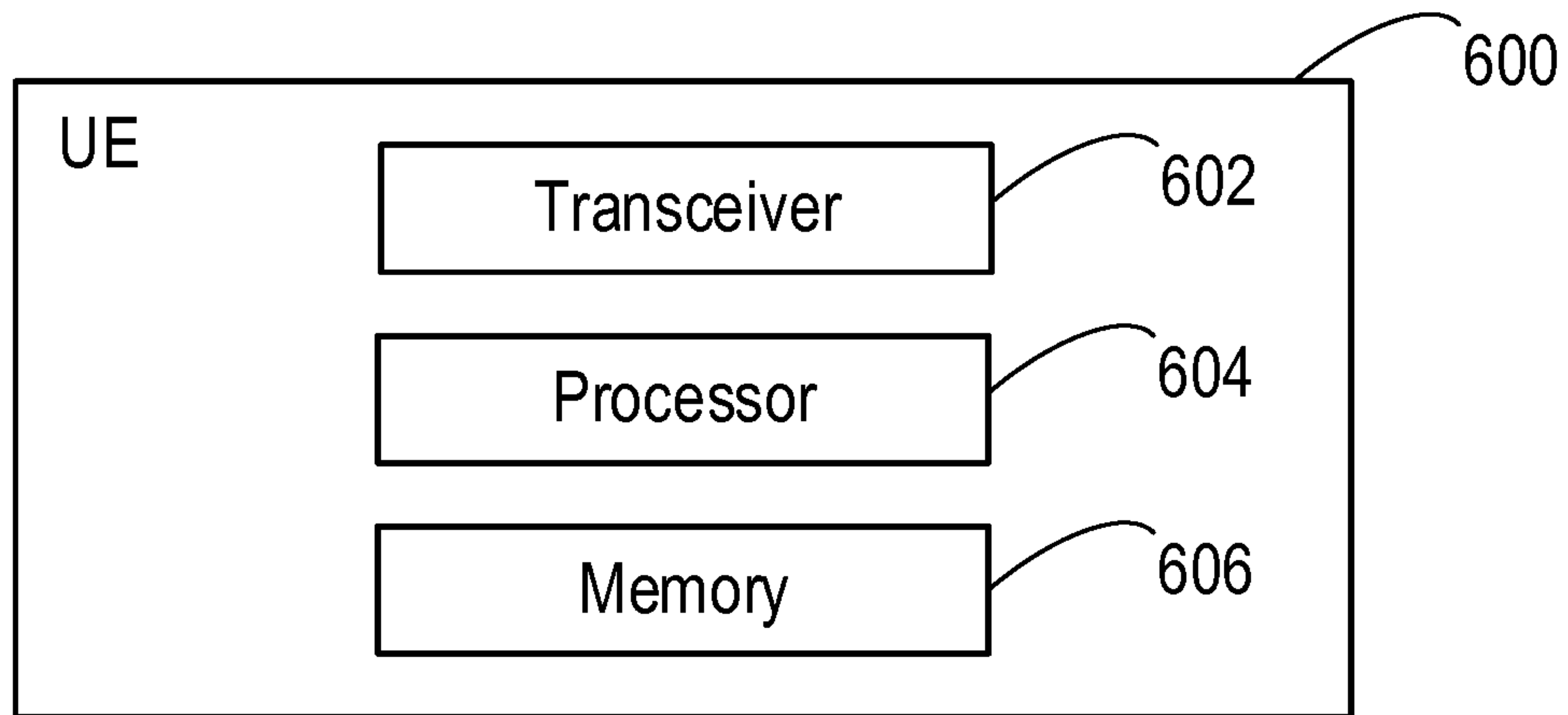


Figure 6

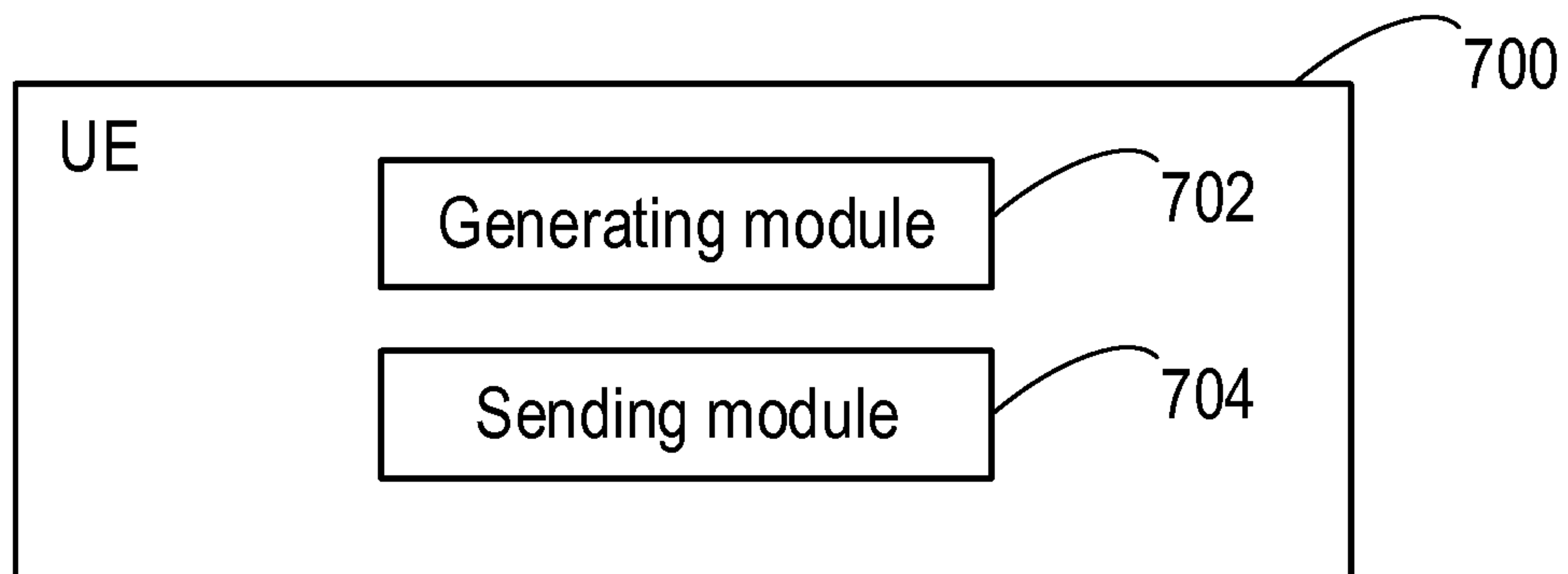


Figure 7

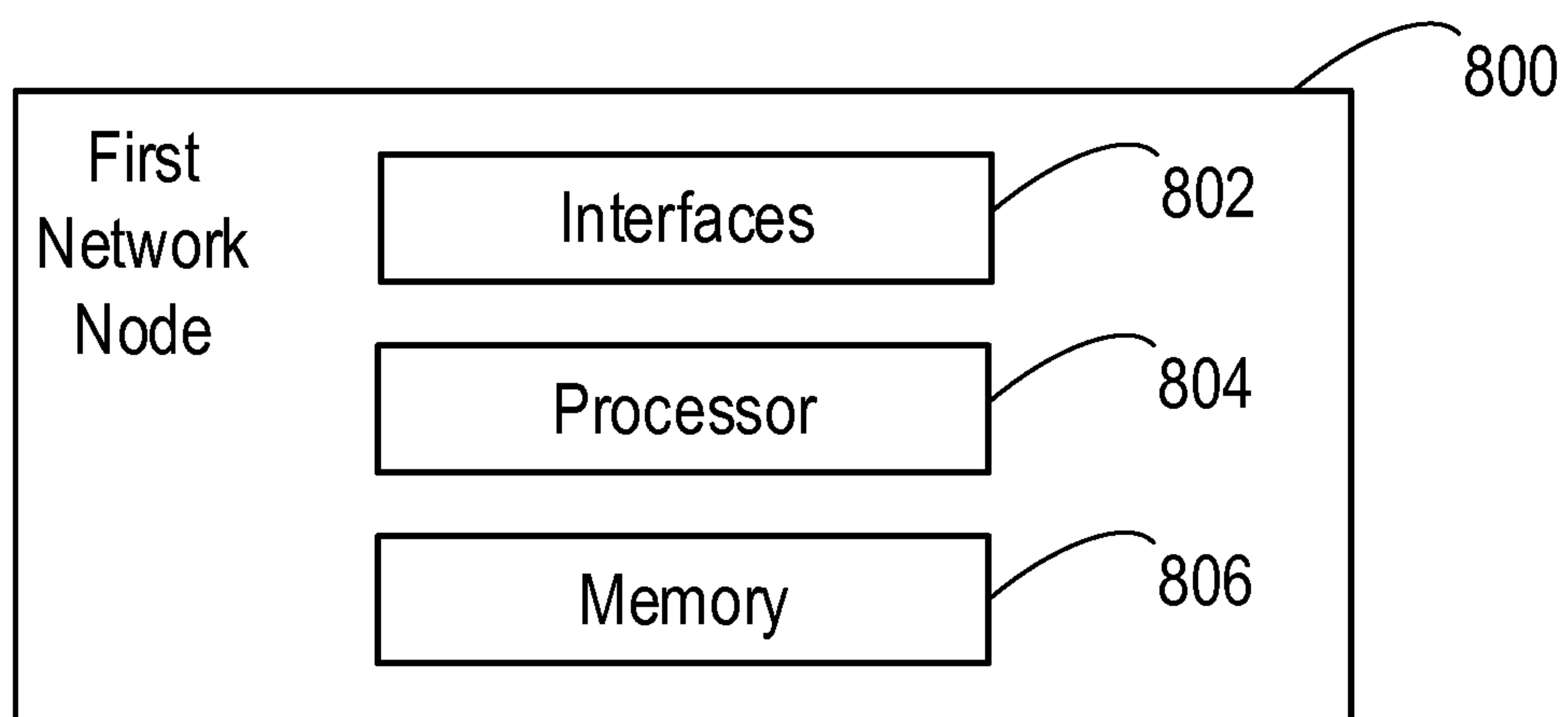


Figure 8

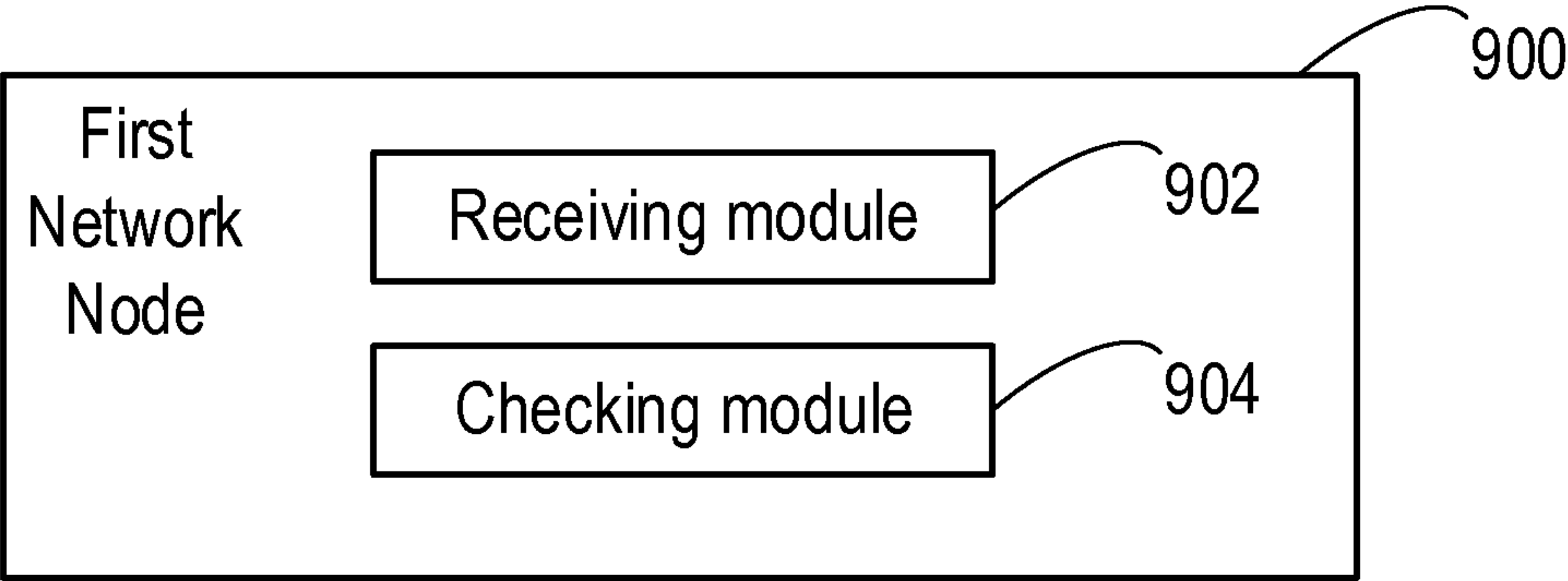


Figure 9

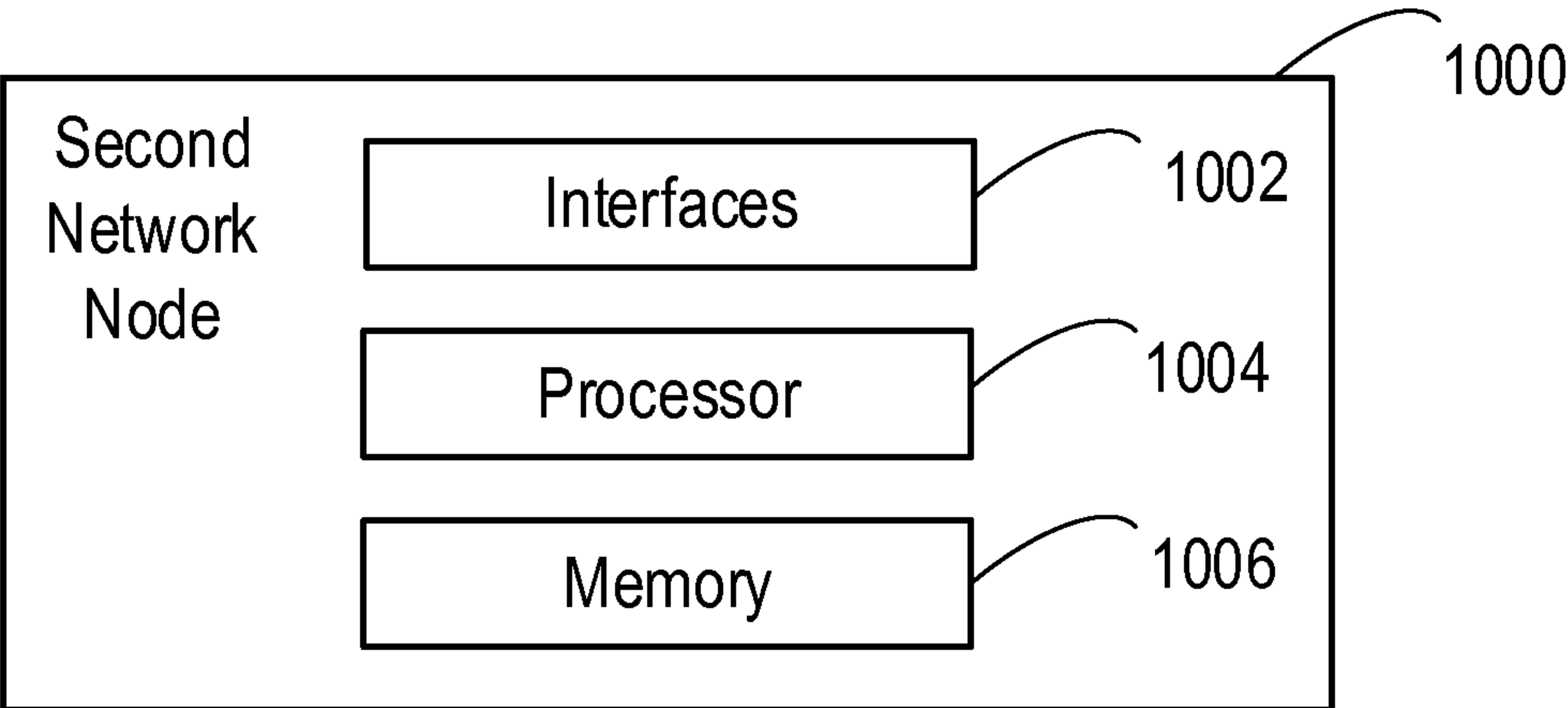


Figure 10

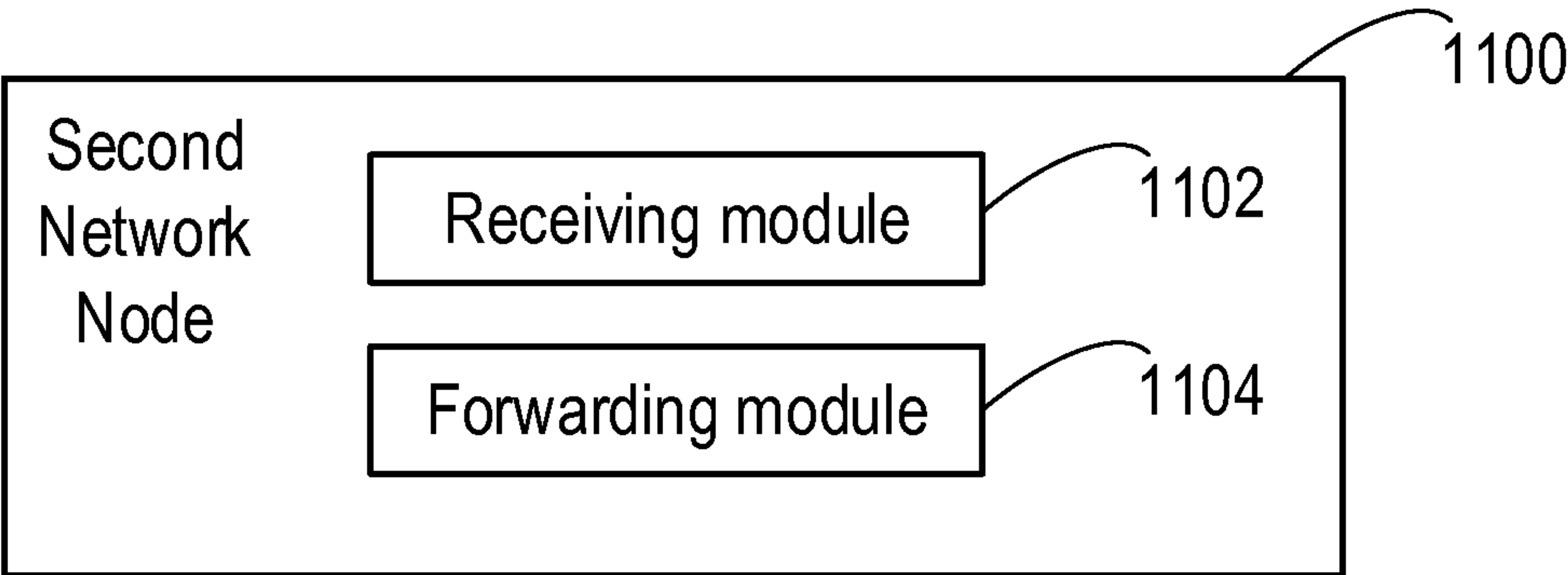


Figure 11

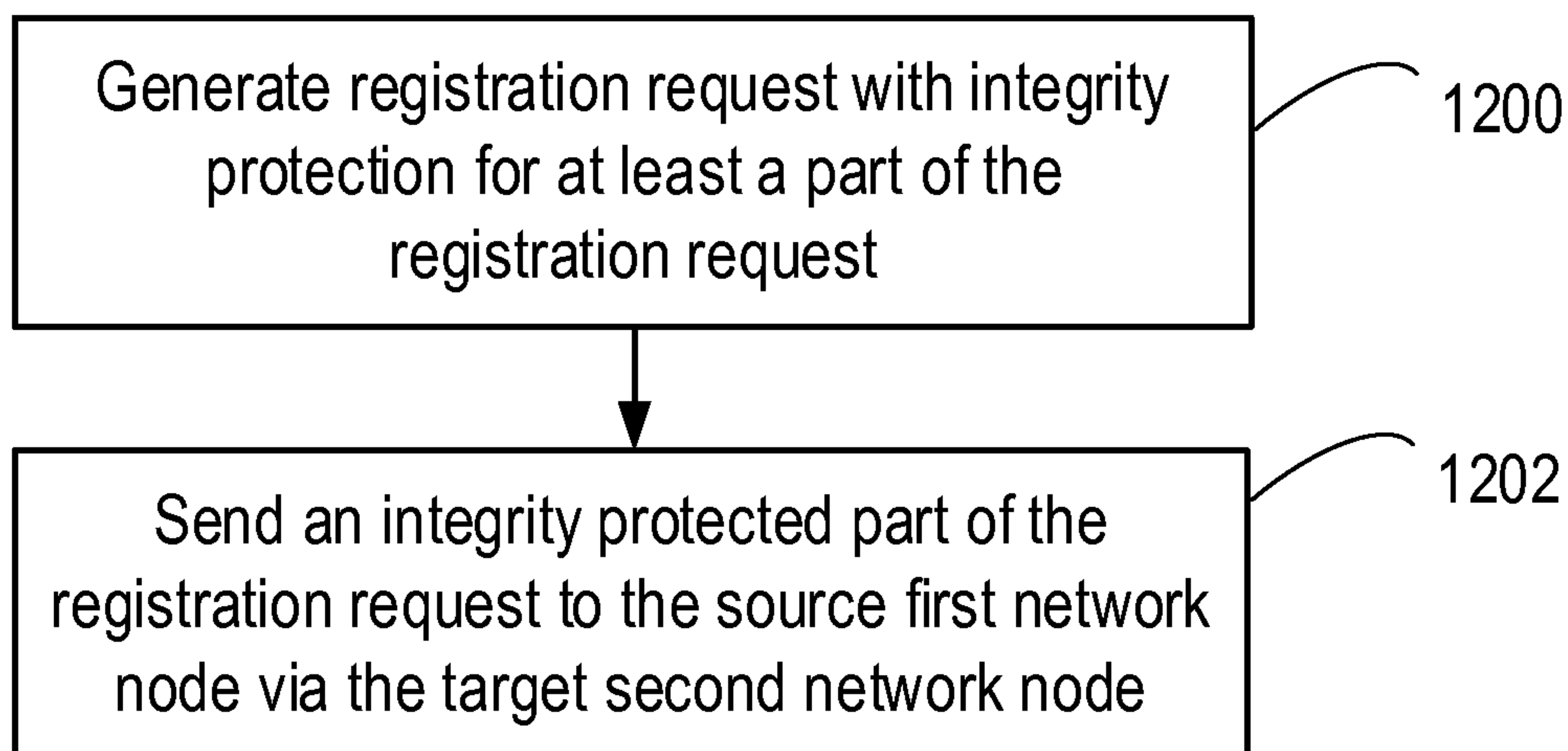


Figure 12

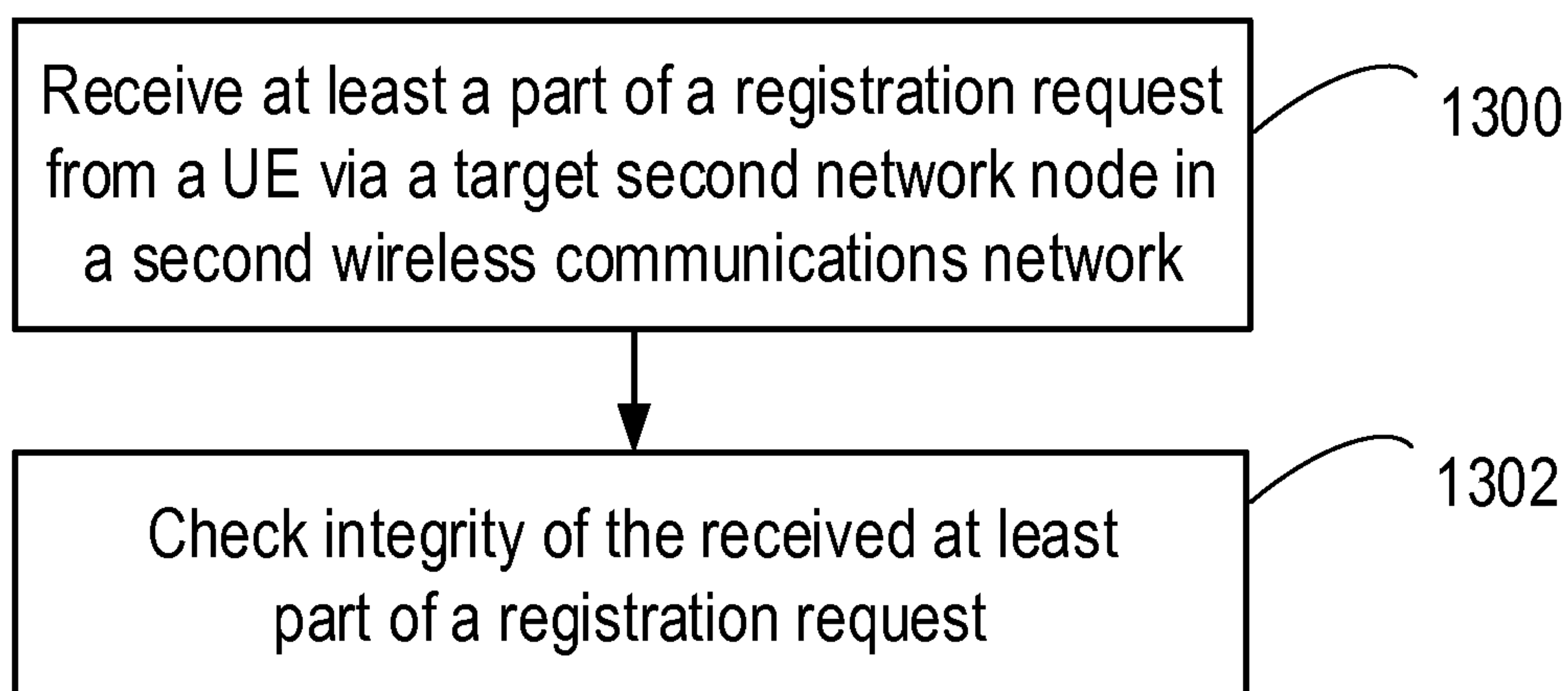


Figure 13

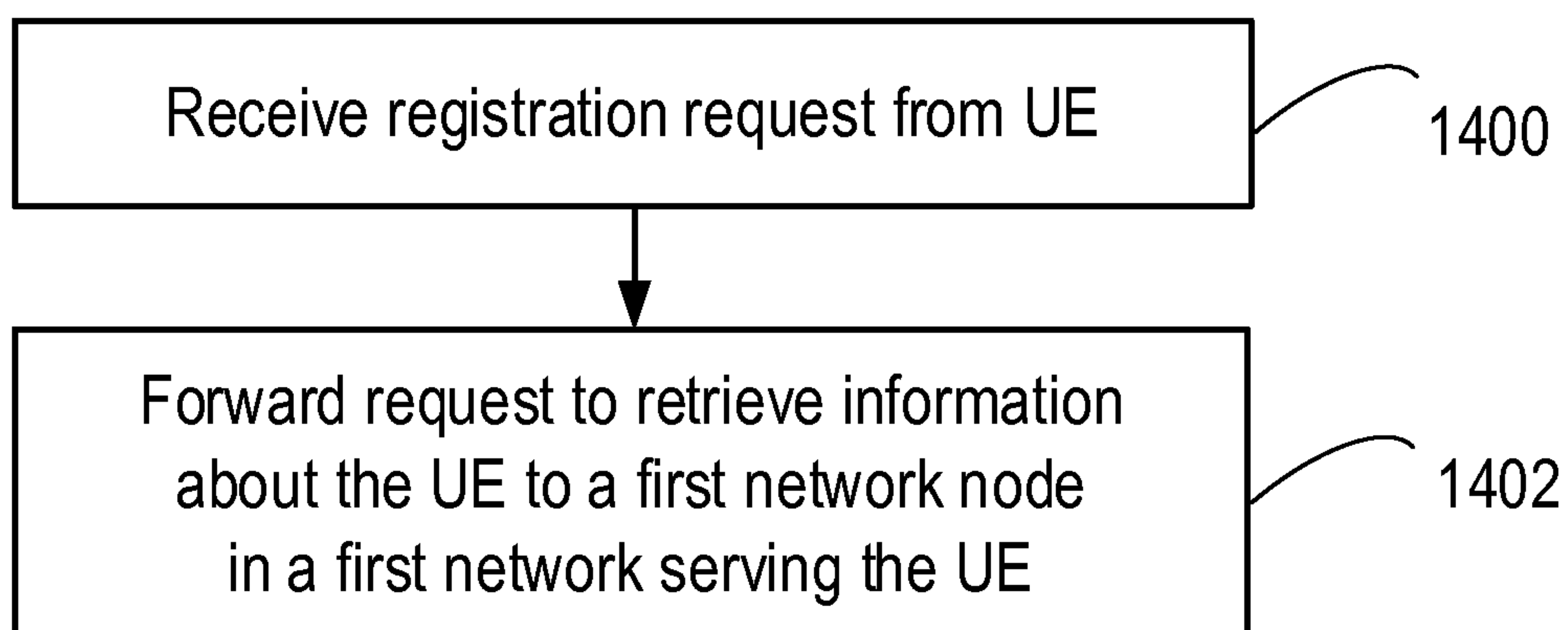


Figure 14

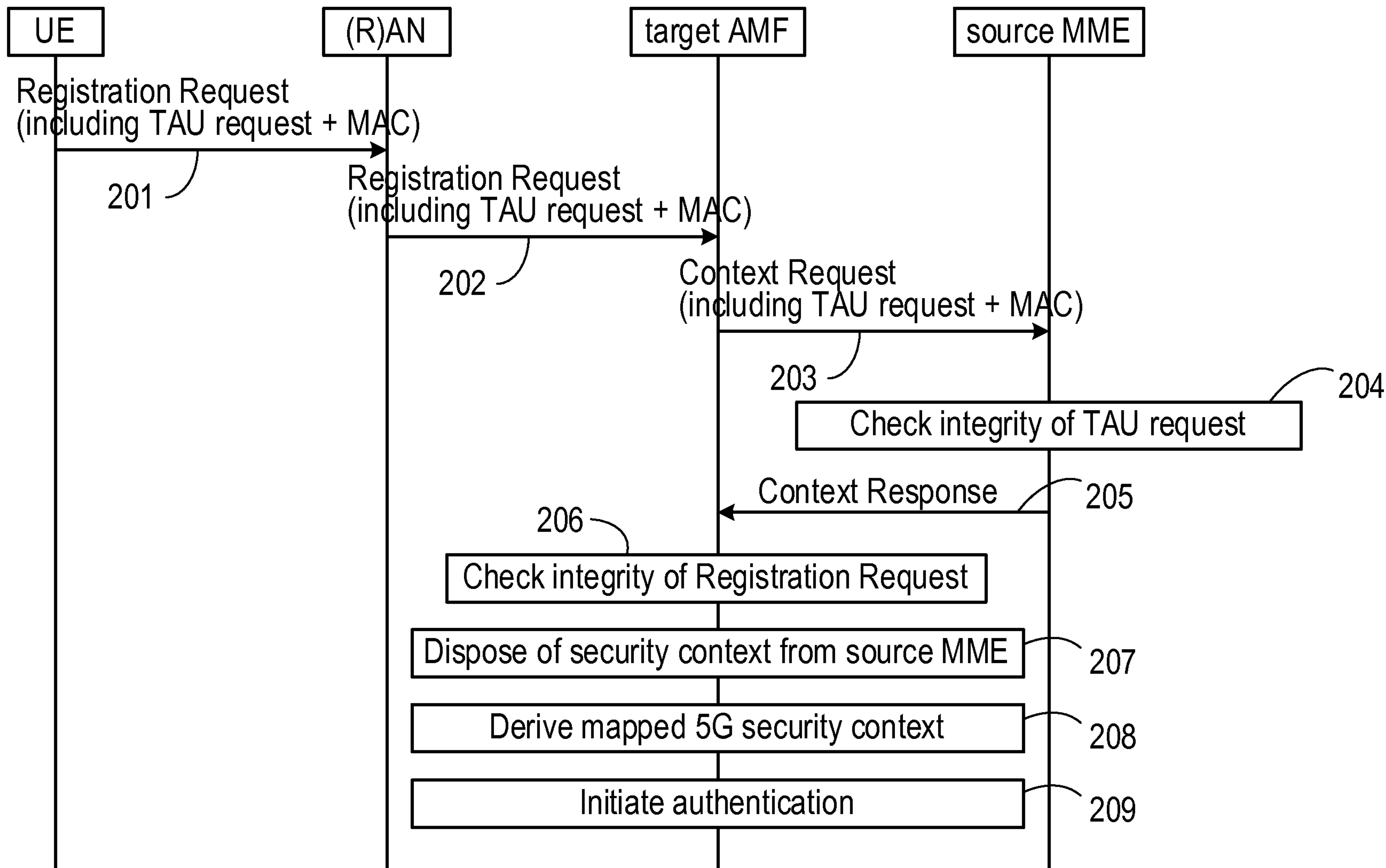


Figure 2