example, a public WLAN or femtocell access network). Trusted access networks include access networks that the network operator considers have a level of trust from a security stand point and may interface directly with the EPC network.

[0006] In the new set of 5G standards, a Non-3GPP Access Network (N3AN) is treated as a 5G Access Network and part of the 5G System (5GS). For untrusted non-3GPP access, a Non-3GPP Interworking Function (N3IWF) provides termination of signaling interfaces for control-plane and user-plane respectively, same as an NG-RAN node. Thus, 5G capable UEs can access the 5G core network (5GCN) by connecting to Non-3GPP Access Network as a 5G Access Network via the N3IWF. The N3IWF relays uplink and downlink control-plane signaling between the UE and the 5GCN. In addition, the N3IWF provides user plane connection between the UE and the 5GCN for sessions over non-3GPP access networks.

[0007] Currently, the signaling procedures between the UE and N3IWF are specified when certain security authentication establishment is accepted by the network. However, there is no method available to handle the case when the security association establishment is not accepted by the network. Similarly, for user plane connections, a method needs to be specified to handle the case when the user plane security association establishment is not accepted by the network.

[0008] Therefore, a need exists to provide a system and method that supports handling failure during security association establishment for access to 5GCN via non-3GPP access networks. Other needs and benefits are also provided with embodiments described herein.

SUMMARY

[0009] The following presents a summary of the disclosed subject matter in order to provide a basic understanding of some aspects of the disclosed subject matter. This summary is not an exhaustive overview of the disclosed subject matter. It is not intended to identify key or critical elements of the disclosed subject matter or to delineate the scope of the disclosed subject matter. Its sole purpose is to present some concepts in a simplified form as a prelude to the more detailed description that is discussed later.

[0009a] In an aspect, the present disclosure refers to an interworking function node for managing a network connection over an untrusted access network to a core network, comprising: a first network interface configured to communicate with user equipment (UE) over the untrusted access network; a second network interface configured to communicate

with one or more nodes in the core network; and a processing device configured to: process a request to establish a secure connection to the core network, received from the UE over the untrusted access network; provide, to the one or more nodes in the core network via the second network interface, an authentication and secure connection establishment request; determine, based upon a response from the one or more nodes in the core network in response to the authentication and secure connection establishment request, that establishment of secure connections over untrusted access networks is not allowed by the core network; provide, to the UE, a response message comprising an indication that the request to establish the secure connection is not approved because connection establishment over the untrusted access network is not allowed by the core network; and receive, from the UE, in response to the response message, a stop message terminating the request to establish the secure connection to the core network.

[0009b] In another aspect, the present disclosure refers to an Access and Mobility management Function (AMF) for handling a network connection request from the interworking function node, comprising: a network interface configured to communicate with an interworking function node and an authentication function in a core network; and a processing device configured to: receive, from the interworking function node, over the network interface, an authentication and secure connection establishment request, the authentication and secure connection establishment request being associated with a request for connection establishment with the core network received by the interworking function node, from a user equipment (UE), over an untrusted access network; in response to receiving the authentication and secure connection establishment request, provide a request for authentication and subscription check towards an Authentication Server Function (AUSF) of the core network; in response to determining that the authentication and subscription check by the AUSF has failed, generate a response message to the authentication and secure connection establishment request received from the interworking function node by encapsulating in the response message a cause value indicating that access to the core network is not allowed over the untrusted access network; and provide the response message to the interworking function node.

[0009c] In another aspect, the present disclosure refers to a user equipment, comprising: a network interface configured to communicate with an interworking function node of a core network over an untrusted access network; and a processing device configured to: generate a registration request for secure session establishment to the core network; send, over the

untrusted access network, to the interworking function node of the core network, the registration request; receive, in response to the registration request, from the interworking function node of the core network, a response message, the response message comprising an indication of whether access to the core network over untrusted access networks is allowed by the core network; determine, from the response message, that the secure session establishment over the untrusted access network is not allowed by the core network; and in an instance in which the secure session establishment over the untrusted access network is not allowed by the core network, providing, to the interworking function node, a stop message to terminate the request for the secure session establishment with the core network.

[0010] In one example, an interworking function node for managing a network connection over an untrusted access network to a core network includes a first network interface configured to communicate with user equipment (UE) over the untrusted access network and a second network interface configured to communicate with one or more nodes in the core network. The interworking function node includes a processing device configured to process a request for a connection establishment to the core network from the UE in the untrusted

access network and generate a request to the core network; determine the connection establishment is not accepted by the core network; and generate a response message to the UE, wherein the response message includes an error indicating that the connection establishment over the untrusted access network is not allowed by the core network.

[0011] In another example, an Access and Mobility Management function (AMF) for handling a network connection request from the interworking function node includes a network interface configured to communicate with an interworking function node and an authentication function in a core network. The AMF also includes a processing device configured to process a request for authentication and secure connection establishment for a UE over an untrusted access network; generate a request for authentication and subscription check towards an Authentication Server Function (AUSF); determine a response for the authentication and subscription check indicates an authentication failure; and generate a response message of authentication and secure connection establishment by including in the response message a cause value indicating access to the core network is not allowed over the untrusted access network.

[0012] In another example, user equipment (UE) includes a network interface configured to communicate with an interworking function node over an untrusted access network. The UE includes a processing device configured to generate a registration request for secure session establishment to a core network; process a response message from the interworking function node; and determine from the response message that the connection establishment over the untrusted access network is not allowed by the core network.

[0013] In one or more of the above examples, the processing device in the interworking function node is configured to receive a request for authentication and secure connection establishment from the UE over the untrusted access network; generate a request for authentication and subscription check and transmit the request for authentication and subscription check over the second interface towards Access and Mobility management Function (AMF); receive a response for authentication and subscription check from the AMF; and generate an Internet Key Exchange (IKE) response message to the UE with an NAS payload including the error indicating that the connection establishment over the untrusted access network is not allowed by the core network.

[0014] In one or more of the above examples, the processing device in the interworking function node is configured to receive a response from the Access and Mobility Management Function encapsulating a Registration Reject message including a 5GMM cause value

indicating Non-3GPP access to 5GCN not allowed and generate an Internet Key Exchange (IKE) response message with the payload including a message type indicating that the connection establishment is not accepted by the core network.

[0015] In one or more of the above examples, the processing device in the interworking function node is configured to generate the Internet Key Exchange (IKE) response message with a notify payload including a private notify message type indicating a failure reason.

[0016] In one or more of the above examples, the processing device in the interworking function node is configured to generate the IKE response message by generating the IKE response message with a notify payload including a private notify message type indicating that untrusted non-3GPP access to the 5GCN is not allowed.

[0017] In one or more of the above examples, the processing device in the interworking function node is configured to transmit the response message to the UE, wherein the response message indicates that the connection establishment is not accepted by the core network; receive a stop message from the UE; and generate a failure message to the UE.

[0018] In one or more of the above examples, the processing device in the interworking function node is configured to process the stop message from the UE, wherein the stop message includes a 5G-Stop message format having a message identifier field and wherein the message identifier field includes a 5G-Stop identifier.

[0019] In one or more of the above examples, the request for the connection establishment from the UE in the untrusted access network includes an IKE request message to initiate an IPsec Security Association (SA) with the core network.

[0020] In one or more of the above examples, the core network is a 5GCN and the untrusted access network is a non-3GPP access network.

[0021] In one or more of the above examples, the processing device in AMF is configured to encapsulate in the response message a Registration Reject message that includes the cause value, wherein the cause value includes a 5GMM cause value indicating Non-3GPP access to the 5GCN is not allowed.

[0022] In one or more of the above examples, the processing device in AMF is configured to generate an Extensible Authentication Protocol (EAP) failure indication in the response message.

[0023] In one or more of the above examples, the processing device in the user equipment is configured to generate a stop message indicating an end to the registration request for

secure session establishment to the 5GCN and transmit the stop message over the non-3GPP access network to the interworking function node.

[0024] In one or more of the above examples, the processing device in the user equipment is configured to generate the stop message as an EAP-Response formatted message including a message identifier field set to 5G-Stop.

[0025] In one or more of the above examples, the processing device in the user equipment is configured to process an EAP failure message from the interworking function node; and perform a security association deletion procedure.

[0026] In one or more of the above examples, the processing device in the user equipment is configured to re-attempt registration with the 5GCN by generating a second registration request for secure session establishment to the 5GCN and determine from a second response message from the interworking function node that the connection establishment over the untrusted access network is successful.

[0027] In one or more of the above examples, the processing device in the user equipment is configured to generate the second registration request for secure session establishment to the 5GCN with updated parameters.

[0028] Additional aspects will be set forth, in part, in the detailed description, figures and any claims which follow, and in part will be derived from the detailed description. It is to be understood that both the foregoing general description and the following detailed description is exemplary and explanatory only, and the claims are not restricted to the embodiments disclosed.

BRIEF DESCRIPTION OF THE SEVERAL VIEWS OF THE DRAWINGS

[0029] Some embodiments of apparatus and/or methods in accordance with embodiments of the disclosure are now described, by way of example only, and with reference to the accompanying drawings, in which:

[0030] FIG. 1 illustrates a schematic block diagram of an embodiment of types of access networks.

[0031] FIG. 2 illustrates a schematic block diagram of an embodiment of a 5G System Architecture for non-3GPP access.

[0032] FIG. 3 illustrates a logical flow diagram illustrating an embodiment of a method for a UE to register to a 5GCN via an untrusted non-3GPP access network.

[0033] FIG. 4 illustrates a logical flow diagram of an embodiment of a method for to handle the case when IKE SA and signalling IPsec SA establishment is not accepted.

CLAIMS

1. An interworking function node for managing a network connection over an untrusted access network to a core network, comprising:

a first network interface configured to communicate with user equipment (UE) over the untrusted access network;

a second network interface configured to communicate with one or more nodes in the core network; and

a processing device configured to:

process a request to establish a secure connection to the core network, received from the UE over the untrusted access network;

provide, to the one or more nodes in the core network via the second network interface, an authentication and secure connection establishment request;

determine, based upon a response from the one or more nodes in the core network in response to the authentication and secure connection establishment request, that establishment of secure connections over untrusted access networks is not allowed by the core network;

provide, to the UE, a response message comprising an indication that the request to establish the secure connection is not approved because connection establishment over the untrusted access network is not allowed by the core network; and

receive, from the UE, in response to the response message, a stop message terminating the request to establish the secure connection to the core network.

2. The interworking function node of claim 1, wherein the processing device is configured to:

receive, from the UE, over the first network interface, the request to establish the secure connection over the untrusted access network;

transmit, over the second network interface, towards the one or more nodes of the core network, the authentication and secure connection establishment request;

receive, from the one or more nodes of the core network, over the second network interface, an authentication and secure connection establishment response ; and

generate an Internet Key Exchange (IKE) response message to the UE with an NAS payload including the indication that the establishment of the secure connection over the untrusted access network is not allowed by the core network.

3. The interworking function node of claim 2, wherein the processing device is further configured to:

receive a response from an Access and Mobility Management Function of the core network, the response including a Registration Reject message including a cause value indicating that access to the core network over the untrusted access network is not allowed; and

generate the IKE response message with the NAS payload including a message type indicating that the connection establishment over the untrusted access network is not allowed by the core network.

4. The interworking function node of claim 2, wherein the processing device is further configured to generate the IKE response message by either:

generating the IKE response message with a notify payload including a private notify message type indicating a failure reason; or

generating the IKE response message with the notify payload including the private notify message type indicating that the connection establishment over the untrusted access network is not allowed by the core network.

5. The interworking function node of any preceding claim, wherein the processing device is further configured to:

transmit the response message to the UE, wherein the response message indicates that the connection establishment over the untrusted access network is not allowed by the core network; and

in response to receiving the stop message from the UE, generate a failure message to the UE.

6. The interworking function node of any preceding claim, wherein the processing device is further configured to:

process the stop message from the UE, wherein the stop message includes a 5G-Stop message format having a message identifier field, and wherein the message identifier field includes a 5G-Stop identifier.

7. The interworking function node of any preceding claim, wherein the request for the connection establishment from the UE in the untrusted access network includes an IKE request message to initiate an IPsec Security Association (SA) with the core network.

8. The interworking function nodes of any preceding claim, wherein the core network is a 5GCN and the untrusted access network is a non-3GPP access network.

9. An Access and Mobility management Function (AMF) for handling a network connection request from the interworking function node, comprising:

a network interface configured to communicate with an interworking function node and an authentication function in a core network; and

a processing device configured to:

receive, from the interworking function node, over the network interface, an authentication and secure connection establishment request, the authentication and secure connection establishment request being associated with a request for connection establishment with the core network received by the interworking function node, from a user equipment (UE), over an untrusted access network;

in response to receiving the authentication and secure connection establishment request, provide a request for authentication and subscription check towards an Authentication Server Function (AUSF) of the core network;

in response to determining that the authentication and subscription check by the AUSF has failed, generate a response message to the authentication and secure connection establishment request received from the interworking function node by encapsulating in the response message a cause value indicating that access to the core network is not allowed over the untrusted access network; and

provide the response message to the interworking function node.

10. The AMF of claim 9, wherein the processing device is configured to:

encapsulate in the response message a Registration Reject message that includes the cause value, wherein the cause value includes a cause value indicating access to the core network over the untrusted access network is not allowed by the core network.

11. The AMF of claim 10, wherein the processing device is configured to:

generate an Extensible Authentication Protocol (EAP) failure indication in the response message.

12. The AMF of any one of claims 9-11, wherein the untrusted access network is a non-3GPP access network and the core network is a 5G core network (5GCN).

13. User equipment, comprising:

a network interface configured to communicate with an interworking function node of a core network over an untrusted access network; and

a processing device configured to:

generate a registration request for secure session establishment to the core network;

send, over the untrusted access network, to the interworking function node of the core network, the registration request;

receive, in response to the registration request, from the interworking function node of the core network, a response message, the response message comprising an indication of whether access to the core network over untrusted access networks is allowed by the core network;

determine, from the response message, that the secure session establishment over the untrusted access network is not allowed by the core network; and

in an instance in which the secure session establishment over the untrusted access network is not allowed by the core network, providing, to the interworking function node, a stop message to terminate the request for the secure session establishment with the core network.

14. The user equipment of claim 13, wherein the processing device is further configured to:

generate the stop message, the stop message indicating an end to the registration request for secure session establishment to the core network.

15. The user equipment of claim 14, wherein the processing device is further configured to:

generate the stop message as an Extensible Authentication Protocol (EAP)-Response formatted message including a message identifier field set to 5G-Stop.

16. The user equipment of claim 15, wherein the processing device is further configured to:

process an EAP failure message from the interworking function node; and

perform a security association deletion procedure.

17. The user equipment of claim 13, wherein the processing device is further configured to:

re-attempt registration with the core network by generating a second registration request for secure session establishment to the core network; and

determine, from a second response message from the interworking function node, that the connection establishment over the untrusted access network is successful.

18. The user equipment of claim 17, wherein the processing device is further configured to:

generate the second registration request for secure session establishment to the core network with updated parameters.

19. The user equipment of any one of claims 13-18, wherein the untrusted access network is a non-3GPP access network and the core network is a 5G core network (5GCN).