

Method and Arrangement in a Telecommunication System

5

TECHNICAL FIELD

The present invention relates to methods and arrangements in a telecommunication system, in particular to methods and arrangements for network-controlled configurations of the link maximum transmission unit (MTU) in a user equipment (UE).

BACKGROUND

Within the 3rd Generation Partnership Project (3GPP) work is currently ongoing on UTRAN long term evolution (LTE). System Architecture Evolution / Long Term Evolution (SAE/LTE) architecture that moves PDCP, user plane ciphering and header compression to the enhanced Node B (eNB) changes the needs for handling the length of S1-U (and X2-U) frames as the length of the S1-U (and X2-U) frame then is considerably increased. Therefore appropriate solutions to deal with the length of Maximum Transmission Unit (MTU) are necessary. At the same time capabilities to minimise the probability of S1-U frame being fragmented have been somewhat increased.

The following problems relate to fragmentation:

Transport overhead: Every fragment includes an additional IP header; hence it adds additional transmission overhead. It is 20 octets (though depending on the usage of optional headers) per fragment and in case of IPv4 and, in case of IPv6, 48 octets (i.e. 40 octets of standard IPv6 header plus 8 octets of the fragment header). A typical transport layer

datagram would be carried in 2 fragments. Therefore, a selection of length of transport layer datagram so that it fits into single IP packet provides significantly lower aggregate overhead.

- 5 Incomplete discard: In case packets are discarded due to congestion it is very likely that fragments of the same datagram are discarded independently. Hence transport network resources are used to forward data that will be discarded at the receiver, the Serving Gateway (SGW) or eNB.
- 10 In case of severe congestion it could lead to further discarding and hence more incomplete datagrams.

Processing efficiency: It is generally accepted that the S1 interface is the bottleneck. Therefore considerable packet loss and delay variation could be present for interactive and best effort flows even in a normal condition in order to maximise the end-user perceived data rate and utilisation of scarce S1 resources. This may require significant processing effort and relatively long-term memory reservation for reassembly of the original datagrams in the receiver as the reassembly buffers have to be allocated for at least for the length of perceived delay variation on the applicable transmission path.

Security threat: It should be noted that typical implementations assume that only fraction of datagrams are fragmented and, if the datagrams are fragmented, the fragments arrive with very short interval. That allows for limitation of the memory required for reassembly. Therefore, transmission of incomplete datagrams is a common way to introduce denial of service attacks as scarce reassembly buffers are consumed for extensive periods and legitimate fragmented datagrams could be discarded due to lack of reassembly buffers/engines. Although this is not really a problem for (logical) SGW and eNB as those nodes use secure network, it could be a problem for security gateways (SEG)

in case the fragmentation is performed on the path between SEG-s.

False reassembly: The identification header used for reassembly is only 16 bits in case of IPv4 (32 bits in case of IPv6). Considering the peak data rate, measured in packets per second, there is high probability of the wrap around of the ID and therefore incorrect reassembly (though this also depends on the setting of the reassembly timer at the receiver). The false reassembly results in at least further data loss that may be detected by the receiver or even an integrity (and potentially confidentiality) violation.

Hence there exists a need for a system architecture that removes or at least reduces the problems relating to fragmentation.

SUMMARY

The path MTU, i.e. the path between application server and the UE in an LTE network, such as the network depicted in Fig. 1, is affected by numerous events. Every link in the IP network has a defined Maximum Transmission Unit (MTU), and so does the link that is used by the IP Host in the UE. It has been observed to be a problem how to configure the link MTU in the UE. Generally, any "reasonable" default value that is updated with path MTU discovery could be initially used.

However, it should be noted that there are number of configurations/implementations (for instance of firewalls/gateways) that discard a number of IPv4 ICMP messages including "Packet Too Big" messages. Hence, it can be assumed that end-to-end path MTU discovery is not used in case of IPv4. This in turn leads to a fragmentation in the

network and all the problems associated with such fragmentation.

In order to overcome the identified problems, the network is set to configure the link MTU in the UE for each bearer
5 where the network-configured link MTU could represent an MTU of a path for a SAE bearer service in complete or part of a particular SAE/LTE network.

When the SAE/LTE nodes are made aware of the MTU supported in the SAE/LTE network, the network can be adapted to
10 configure the link MTU in the UE so that the fragmentation in the SAE/LTE network can be avoided or at least the probability reduced significantly. If that MTU is made available to the host in the UE, the stack in the UE is enabled to provide the following behaviour that reduces the
15 need for fragmentation in the network significantly:

- in case of transport layer protocol that has a Maximum Segment Size (MSS), e.g. Transmission Control Protocol (TCP) or Stream Control Transmission Protocol (SCTP), both the transmit and receive MSS can be selected by the UE
20 considering the link MTU configured by the network and hence fragmentation can be avoided altogether (or at least in the SAE/LTE network domain); In case of TCP receive MSS can be signalled to the peer in SYN and SYN ACK messages at the establishment of the TCP connection.

- 25 - in case of a transport layer protocol that does not have a Maximum Segment Size (MSS), e.g. UDP, the UE may fragment the transmitted datagram at the source according to the link MTU configured by the network and hence fragmentation can be avoided at least in the uplink direction.

30 The invention also extends to nodes in a SAE/LTE network configured to transmit the link MTU to a UE and also to a UE configured to receive the link MTU and to base transmission on the link MTU.

Hence in accordance with the present invention the MTU supported by the SAE/LTE network is signalled to the UE.

5 One advantage of the present invention is that the UE is enabled to use the optimised MTU for SAE/LTE network without adding significant additional complexity. Furthermore, allowed time-constraints for an increase of the MTU via path MTU discovery effectively do not allow to take advantage of
10 changes in path MTU due to mobility (i.e. the evolved Node Bs (eNB-s) between which the UE is moving may be connected to different IP networks with different MTU). Handovers are considered in a mobile network significantly more frequently than defined timing constraints for path MTU discovery.

15 BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 illustrates the impact on the path MTU from SAE/LTE protocol architecture on S1-U.

Figure 2 illustrates SAE bearer establishment/ modification.

Figure 3 illustrates radio bearer establishment/
20 modification.

DETAILED DESCRIPTION

As mentioned above, the path MTU, i.e. the path between application server and the UE, as depicted e.g. in figure 1, can be affected by numerous impacts including:

- 25 - Uncompressed header of original (i.e. end-to-end user) IP-packets;
- The S1-U tunneling protocol (GTP-U);

- IPSec tunnel (Encapsulating Security Payload (ESP) Security Association (SA) in tunnel mode) for integrity and confidentiality protection in the access network between security gateways (SEG);

5 - An MTU provided by the data link layer on particular instance of S1 interface;

- An MTU imposed on a particular administrative (and QoS) domain of the IP network;

10 The used version of the Internet Protocol (i.e. IPv4 or IPv6).

Aspects described in some of the problems above could introduce a variable path MTU primarily due to user mobility. Another source of variable path MTU can be link failures and the following re-routing in the IP network.

15 Moreover, it is very likely that the SAE/LTE network has the shortest MTU on the end-to-end path.

Every link in the IP network has a defined MTU, and so does the link that is used by the IP Host in the UE. It has been observed to be a problem how to configure the link MTU in the UE. Generally, any reasonable default value that is

20 updated with path MTU discovery could be initially used. However, it should be noted that there are number of configurations/implementations (for instance of firewalls/gateways) that discard the number of IPv4 ICMP messages

25 including "Packet Too Big" type of messages. Hence, it can be assumed that end-to-end path MTU discovery is not used in case of IPv4. This in turn leads to a fragmentation in the network and all the problems associated with such fragmentation. The fragmentation in case of a deployment as

30 illustrated in figure 1 can occur on different levels including fragmentation of end-to-end datagram,

fragmentation of S1-U datagram, fragmentation of IPSec tunnel datagram.

If the SAE/LTE nodes are made aware of the MTU supported in the SAE/LTE network, the network is enabled to configure the link MTU in the UE such that the fragmentation in the SAE/LTE network can be avoided or at least significantly reduced. If this MTU is available to the host in the UE, the stack in the UE is able to provide the following behaviour for reducing the need of fragmentation in the network:

10 In case of a transport layer protocol that has a Maximum Segment Size MSS e.g. TCP both the transmit and receive MSS can be selected by the UE considering the "link" MTU configured by the network and, hence, fragmentation can be avoided altogether or at least in the SAE/LTE network domain.

In case of a transport layer protocol that does not have a Maximum Segment Size (MSS) e.g. UDP the UE can fragment the transmitted datagram at the source according to the "link" MTU configured by the network and, hence, fragmentation can be avoided at least in the uplink direction.

In accordance with the present invention the MTU supported by the SAE/LTE network is signalled to the UE.

The following describes by means of non-exclusive examples different embodiments for signalling of the link MTU.

25 In accordance with a first embodiment the link MTU is signalled in a Non Access Stratum (NAS) message from the Mobility Management Entity (MME). As the signalled link MTU conceptually represents the MTU supported by the SAE bearer service it is expressed explicitly. The NAS signalling for SAE bearer establishment and modification is illustrated in figure 2. Hence first in a message 201 a Non Access Stratum (NAS) message from the Mobility Management Entity (MME)

including a SAE Bearer Setup/ Modification Request and the link MTU. In response to the message 201 the UE transmits a NAS message 203 acknowledging that the SAE Bearer Setup/Modification is completed.

- 5 In accordance with one embodiment of the present invention, the MME signals in the NAS SAE bearer setup/modification request message (or a similar message) signals the link MTU that can represent an MTU of a path for a SAE bearer service in a complete or in a part of a particular SAE/LTE network.
- 10 The signalled link MTU can for instance be set to the highest value supported by the SAE/LTE network such that the network does not need to perform IP fragmentation of the original end-to-end datagram or any of the (nested) tunnelling datagrams encapsulating the end-to-end datagram.
- 15 Once the UE receives the link MTU for a particular SAE bearer at SAE bearer establishment or modification, the UE can apply the signalled link MTU for the particular SAE bearer.

- In accordance with another embodiment of the present
- 20 invention, the link MTU is signalled in a Radio Resource Control (RRC) message from an evolved Node B (eNB). The signalled link MTU can for example be part of the radio bearer establishment/modification procedure and can, then, only implicitly represent the MTU supported by the SAE
- 25 bearer service.

- The RRC signalling for Radio bearer establishment and reconfiguration is illustrated in figure 3. In accordance with one embodiment of the present invention, the eNB signals in the RRC Radio bearer setup/reconfiguration
- 30 request message 301 (or a similar message) the link MTU that can implicitly represent an MTU of a path for SAE bearer service in a complete or in a part of a particular SAE/LTE network as known to an eNB. The signalled link MTU can for instance be set to the highest value supported by the

SAE/LTE network so that the network does not have to perform IP fragmentation of the original end-to-end datagram or any of the (nested) tunnelling datagrams encapsulating the end-to-end datagram. Once the UE receives the link MTU for a particular radio bearer at Radio bearer establishment or reconfiguration, the UE is preferably set to apply the signalled link MTU for the particular SAE bearer. Also in response to the message 303 the UE acknowledges that the Radio Bearer Setup/ Reconfiguration is completed.

10 When configuring a domain MTU in the SGW and the eNB, the link MTU is also a property of the administrative domain the link belongs to. Typically this will result in that the least capable link defines the MTU for the complete domain. In addition, it can be assumed that very short MTU-s are not used in modern IP networks. Therefore, the minimum link MTU of S1-U (X2-U) can be generally assumed to be in about 1500 octets minus the applicable overhead. In accordance with one embodiment of the present invention, the eNB-s having defined X2-interfaces between themselves are set to belong to the same administrative domain of an IP network. Similarly the corresponding S1-U instances in the UPE are preferably made part of the same administrative domain.

20 Moreover, in order to avoid small variations of the MTU that can result in worse performance in order to gain a few octets for specific link, it is preferred to configure the MTU of the administrative domain for each corresponding link in the eNB and the UPE. One reason to configure the MTU of the administrative domain for each corresponding link in the eNB and the SGW is because a "too big packets" functionality may be implemented in eNB and UPE as is described below.

There are three fragmentation methods:

Fragmentation of end-to-end IP packet: This option is possible only in case of IPv4 and only in case the "do not

fragment" (DF) bit has not been set. However, there are number of implementations that do fragmentation even if the DF bit has been set. Fragmentation when the DF bit has been set is for example sometimes used to overcome the
5 limitations to run path MTU discovery in IPv4 networks.

The benefit of using the fragmentation of end-to-end IP packet, independent of setting of DF bit as described above, is that the reassembly is pushed to the end-hosts and hence network resources are not spent on reassembly. This is
10 applicable only in case SGW and eNB are configured with the link MTU that corresponds to the S1-U (X2-U) path MTU or if path MTU discovery is used on S1-U (X2-U). Additionally, the hosts terminating the end-to-end flow may do the fragmentation/reassembly by themselves according to the link
15 MTU configured for the link associated with the hosts.

Fragmentation of S1-U (X2-U) tunnelling IP-packets: If fragmentation is a solution used to handle "too big packets" then fragmentation of S1-U (X2-U) tunnelling IP-packets is a preferred option if end-to-end flow is IPv6 flow. It may
20 also be applied in case of IPv4 end-to-end flows.

Furthermore, the fragmentation may be left to the node that interfaces the link with the lowest MTU on the S1-U (X2-U) path in case of IPv4 path on S1-U (X2-U). In case S1-U (X2-U) is IPv6 path then the fragmentation can be performed by
25 the eNB/SGW. However, it should be noted that the most processing and memory intensive process is reassembly and it is therefore performed in eNB/SGW and for very large number of flows.

Fragmentation of IPSec tunnelling IP-packet: The principle
30 is almost the same as for fragmentation of S1-U (X2-U) tunnelling IP-packets. However, one difference is that the reassembly has to be performed in a security gateway (SEG) while the fragmentation may be performed in the node that interfaces with the link with the lowest MTU on the S1-U

(X2-U) path in case of IPv4 IPSec tunnel while it has to be performed by the SEG in case of IPv6 IPSec tunnel.

Moreover, MTU discovery can be divided into different types of MTU discovery, namely end-to-end path MTU discovery, S1-U
5 (X2-U) path MTU discovery, and SEG-to-SEG path MTU discovery.

For end-to-end path MTU discovery the IP hosts terminating the end-to-end IP flow may run Path MTU discovery. However, it should be noted that there are number of configurations/
10 implementations (of firewalls/gateways) that discard the number of IPv4 ICMP messages including "Packet Too Big" messages. Hence it can be assumed that end-to-end path MTU discovery is not used in case of IPv4.

On the other hand in case of IPv6, hosts have the two
15 options either to use MTU of 1280 octets (i.e. the minimum MTU each IPv6 capable node has to support) or to use end-to-end path MTU discovery. Considering the problems related to path MTU discovery for TCP it is preferred to apply common S1-U (X2-U) path MTU in the complete administrative domain
20 of eNB-s anyway in order to avoid change of end-to-end path MTU due to mobility. It should be noted that if common MTU is not applied in the administrative domain of eNB-s then allowed time-constraints for increase of MTU effectively disable the gains from "variable" MTU in the administrative
25 domain as the handovers are several magnitudes more frequent.

For S1-U (X2-U) path MTU discovery, the eNB and SGW may use path MTU discovery instead of administratively configured S1-U (X2-U) path MTU. As S1-U (X2-U) are defined to use
30 trusted networks, it can also be assumed that the operator has direct or indirect control over the handling of ICMP messages and hence path MTU discovery can be used

independent of version of IP used for S1-U (X2-U) tunnelling.

For SEG-to-SEG path MTU discovery, the SEG may use path MTU discovery instead of administratively configured tunnel MTU.

- 5 However it may only be used in case of IPv6 IPSec tunnel as it can not rely on the "Packet Too Big" ICMP messages in case of IPv4 tunnel.

The eNB may be configured with the link MTU according to the MTU of the administrative domain it belongs to. Furthermore,
10 it could be considered that the MME is aware of the configured link MTU in the eNB. If that MTU would be available to the host in the UE, the IP stack in the UE can provide the following behaviour that reduces the need for fragmentation in the network significantly.

- 15 In case of a transport layer protocol that has a MSS, e.g. TCP, both the transmit and receive MSS can be selected by the UE considering the "link" MTU configured by the network and hence fragmentation can be avoided altogether (or at least in the SAE/LTE network domain). In case of a transport
20 layer protocol that does not have MSS, e.g. UDP, the UE may fragment the transmitted datagram at the source according to the "link" MTU configured by the network and hence fragmentation can be avoided at least in the uplink direction.

- 25 Considering the gains provided by configuring the "link" MTU in the UE according to the MTU of the administrative domain the eNB belongs to where the SAE bearer is established to the UE, it is recommended to provide functionality to configure the "link" MTU at the establishment/modification
30 of SAE bearer (e.g. included in NAS: SAE bearer establishment/modification) according to the S1-U path MTU known to the MME for respective eNB.

CLAIMS

1. A method of configuring the link maximum transmission unit (MTU) in a user equipment (UE) adapted to connect to an System Architecture Evolution / Long Term Evolution
5 (SAE/LTE) radio network, **characterized by** the step of signalling the MTU supported by the SAE/LTE network to the UE in one of a Non Access Stratum (NAS) message from a Mobility Management Entity (MME) and a Radio Resource Control (RRC) message from an evolved Node B (eNB).
10
2. The method according to claim 1, when a transport layer protocol of the link has a Maximum Segment Size (MSS), **characterized in** that the transmit and/or the receive MSS are selected based on the MTU signalled to the UE.
15
3. The method according to claim 2, **characterized in** that the transport layer protocol supports signaling of receive MSS and selection of transmit MSS.
- 20 4. The method according to claim 2, **characterized in** that the transport layer protocol is Transmission Control Protocol (TCP) or Stream Control Transmission Protocol (SCTP),
- 25 5. The method according to claim 1, when a transport layer protocol of the link lacks signalling of receive Maximum Segment Size (MSS), **characterized in** that the UE is configured to allow fragmentation of a transmitted datagram at the source based on the MTU signalled to the UE.

6. The method according to claim 5, **characterized in** that the transport layer protocol is UDP.

5 7. The method according to any of claims 1 - 6, **characterized in** that the signalled link MTU is set to the highest value supported by the SAE/LTE network.

8. A user equipment (UE) adapted to connect to a System
10 Architecture Evolution / Long Term Evolution (SAE/LTE) radio network and, **characterized by** means for receiving data comprising the link maximum transmission unit (MTU) supported by the SAE/LTE network, said means comprising one of means for receiving the link MTU in a Non Access Stratum
15 (NAS) message and means for receiving the link MTU in a Radio Resource Control (RRC) message.

9. The user equipment (UE) according to claim 8, **characterized by** means for selecting a transmit and/or
20 receive Maximum Segment Size (MSS) of the transport layer protocol based on the MTU signalled to the UE.

10. The user equipment (UE) according to claim 8, **characterized by** means for allowing fragmentation of a
25 transmitted datagram at the source based on the MTU signalled to the UE.

11. A node in a System Architecture Evolution / Long Term Evolution (SAE/LTE) radio network, **characterized by** means

for signalling the MTU supported by the SAE/LTE network to a User Equipment (UE) connected to the network, said means comprising one of means for signalling the link MTU in a Non Access Stratum (NAS) message and means for signalling the link MTU in a Radio Resource Control (RRC) message.

5

12. The node according to claim 11, **characterized by** means for setting the signalled link MTU to the highest value supported by the SAE/LTE network.

10