3GPP TSG SA WG3 Security — AD Hoc NDS **S3z000012**

8-9 November, 2000

Munchen, Germany

Source: **Siemens**

Title: **Integrity-protection for GERAN-signalling**

Document for: **Discussion**

Agenda Item: **GERAN-security**

Abstract

This contribution proposes GERAN integrity-protection for time-critical messages (such as handoff) that allows for minimal failure rate and an optimal use of the radio spectrum without dropping the security level.

1 Introduction

Integrity protection of signalling messages is part of the work plan for GERAN security, whose overall goal is to provide GERAN with a security level as close to that of UMTS as possible. The security feature ‘integrity-protection’ protects against attacks that exploit unauthorised modification or replay of signalling messages exchanged over the radio interface.

The application of integrity protection requires, besides negotiation of an integrity algorithm and the setting at both sides of the input values, that to each signalling message a message authentication code be added. In UMTS this code is referred to as MAC-I and has a length of 32 bits. In contribution to the overall goal stated above, also the GERAN message authentication code is expected to be 32 bits long.

2 Problem description

In GERAN however, unlike in UMTS, radio resource for signalling messages is provided in discrete amounts, called radio blocks (UTRAN puts no limits to the message size). Signalling messages usually fit into one radio block. Longer signalling messages require segmentation. Segmentation requires more radio resource and more time. Some "unprotected" signalling messages fill up a radio block almost entirely and adding an extra 32 bits for integrity would require segmentation, requiring that it takes more radio resource and more time for the signalling message to be transferred. Sometimes, such as in the event of an handoff, time is critical, and in those cases segmentation will lead to a higher failure rate of those events.

Another problem is that radio resource must have been allocated beforehand. For downlink messages, this does not cause problems, as the network is the sender and is in control of the allocation of radio resource. In uplink however, the mobile equipment cannot use segmentation freely as it does not control the uplink radio resource - and if the network has not allocated the necessary resource, segmentation in uplink is impossible.

3 Proposed solution(s):

For certain signalling messages, integrity protection should be made optional or disabled, or it must be allowed that the message authentication code is shorter than 32 bits. This should apply at least to those signalling messages sent in uplink by the mobile equipment that are *time-critical* and that can be sent *unsegmented* when sent unprotected and require segmentation when protected. But it is mandatory to apply integrity protection whenever it is possible, means when the message authentication code can be added without requiring the segmentation of the message.

In case the option for MAC-I lengths shorter than 32 bits is introduced, such messages must include a field that defines the length of the message authentication code (e.g., a two-bit identifier that allows for the values 8, 16, 24 and 32).

The sender of such a message shall apply integrity protection whenever possible given the Radio resource restriction but may append a shorter message authentication code but always the biggest possible MAC-I that still fits. The receiver of such a not-protected message shall accept the message and act upon it.

As a second part of the proposed mechanism, when the receiver is the network, i.e., precisely in the event of uplink messages, the network may (or must) trigger an in-call local authentication dialogue. This dialogue allows the network to verify that it is still connected with the genuine subscriber and that no radio resource has been stolen. This in-call local authentication dialogue may be optional. We recommend that it be recommended - if not mandated - in the event ciphering is not enabled. The network may trigger such an in-call local authentication dialogue only after the number of consecutive signalling messages that are not protected (or have a shorter message authentication code) exceeds a certain threshold set by the network operator.

As a further extension the mechanism may also be applied to messages that are already segmented, in order to avoid further segmentation.

4 Further steps

TSG GERAN shall define the set of time-critical messages for which the selected mechanism shall apply. All other signalling messages shall be processed with 32-bit MAC-I.