Internal distribution code:

(A) [-] Publication in OJ
(B) [-] To Chairmen and Members
(C) [-] To Chairmen
(D) [X] No distribution

Datasheet for the decision of 23 September 2015

Case Number: T 0981/12 - 3.5.05

Application Number: 06751673.2

Publication Number: 1875656

IPC: H04L9/12, H04L1/18, H04L29/06, H04Q7/38

Language of the proceedings: EN

Title of invention:
Method and apparatus for ciphering and re-ordering packets in a wireless communication system

Applicant:
QUALCOMM INCORPORATED

Headword:
Encryption and numbering of packets/QUALCOMM

Relevant legal provisions:
EPC Art. 56

Keyword:
Inventive step - (no)

Decisions cited:

Catchword:

Europäisches Patentamt
European Patent Office
Office européen des brevets

Beschwerdekammern
Boards of Appeal
Chambres de recours

European Patent Office
D-80298 MUNICH
GERMANY
Tel. +49 (0) 89 2399-0
Fax +49 (0) 89 2399-4465

Case Number: T 0981/12 - 3.5.05

D E C I S I O N
of Technical Board of Appeal 3.5.05
of 23 September 2015

Appellant: (Applicant)	QUALCOMM INCORPORATED 5775 Morehouse Drive San Diego, CA 92121 (US)
Representative:	Heselberger, Johannes Bardehle Pagenberg Partnerschaft mbB Patentanwälte, Rechtsanwälte Prinzregentenplatz 7 81675 München (DE)
Decision under appeal:	**Decision of the Examining Division of the European Patent Office posted on 5 December 2011 refusing European patent application No. 06751673.2 pursuant to Article 97(2) EPC.**

Composition of the Board:

Chair	A. Ritzka
Members:	P. Cretaine
	F. Blumer

Summary of Facts and Submissions

I. This appeal is against the decision of the examining division announced in oral proceedings held on 22 November 2011, with reasons dispatched on 5 December 2011, refusing European patent application No. 06 751 673.2 on the ground of lack of novelty (Article 54 EPC), having regard to the disclosure of

D1: US 2002/0164029.

II. Notice of appeal was received on 7 February 2012. The appeal fee was paid on the same day. A statement setting out the grounds of appeal was received on 2 April 2012. The appellant (applicant) requested that the decision of the examining division be set aside and that a patent be granted on the basis of the claims submitted with the statement setting out the grounds of appeal.

In addition, oral proceedings were requested as an auxiliary measure.

III. A summons to oral proceedings scheduled for 23 September 2015 was issued on 10 July 2015. In an annex to this summons pursuant to Article 15(1) RPBA the board gave its preliminary opinion on the appeal. In particular, the board indicated that the claims did not meet the requirements of Article 56 EPC, having regard to the disclosure of D1 in combination with

D3: EP 0 714 180 or

D4: US 2002/0025820.

IV. With a letter of reply dated 24 August 2015, the appellant submitted an amended page 2a of the description and provided further arguments in respect of inventive step.

V. Oral proceedings were held on 23 September 2015. The appellant's final requests were that the decision under appeal be set aside and that a patent be granted on the basis of the sole request (claims 1 to 34) as filed with the statement setting out the grounds of appeal on 2 April 2012.

VI. At the end of the oral proceedings, the decision of the board was announced.

VII. Claim 1 of the sole request reads as follows:

"A system comprising:
means for ciphering input packets at an access gateway (130) to obtain ciphered packets, each input packet being ciphered with a full sequence number; and
means for generating output packets at a base station (120) for the ciphered packets, each output packet including a partial sequence number used for re-ordering and to decipher the output packets by a receiving entity, wherein each partial sequence number is derived from the full sequence number of a corresponding ciphered packet"

Independent claim 14 of the sole request reads as follows:

"An apparatus comprising:
means for receiving packets ciphered at an access gateway (130) with a full sequence number from at least one base station (120) in a wireless communication

system, each received packet including a partial sequence number derived from the full sequence number and used for re-ordering;
means for deciphering the received packets using the partial sequence number included in each received packet; and
means for re-ordering the received packets based on the partial sequence number included in each received packet."

The request comprises further independent claims directed to corresponding methods and program (claims 11, 27 and 34).

Reasons for the Decision

1. The appeal is admissible.

2. Prior art

2.1 D1 relates to a ciphered communications protocol between a base station and a mobile station in a wireless network (see Figure 1). D1 acknowledges as prior art a protocol having three transmission modes: acknowledged mode AM, unacknowledged mode UM, and transparent mode TM. In the modes AM and UM, the base station associates a sequence number FN to the packets (see paragraphs [0005] and [0010]). To encrypt the packets, the base station uses as encryption key a count-c value formed of a hyper-frame number HFN as the most significant bits and the FN number of the packet as the least significant bits. The HFN number is not transmitted with the encrypted packet, whereas the FN

number is transmitted. The HFN and FN numbers must be synchronised on both mobile and base stations. Therefore, D1 discloses, using the wording of the claims:

- means for ciphering input packets at a base station to obtain ciphered packets, each input packet being ciphered with a full sequence number (see paragraph [0010]: packets input to a first station are encrypted with a count-c value; the count-c value comprises a hyper-frame number HFN and a frame number FN, and represents a full sequence number in the sense of claim 1 of the present application), and

- means for generating output packets at the base station for the ciphered packets, each output packet including a partial sequence number used for re-ordering and to decipher the output packets by a receiving entity, wherein each partial sequence number is derived from the full sequence number of a corresponding ciphered packet (see paragraph [0005]: each packet has a sequence number to explictly indicate the sequential order of each packet within the stream of transmitted packets and the FN value thus represents a sequence number; see paragraph [0010]: the encrypted packets are sent to the second station together with their FN value; see paragraph [0010]: the encrypted packets are decrypted using the count-c value; therefore the FN value represents a partial sequence number in the sense of claim 1 of the present application).

The board notes that the appellant has not rebutted the above assessment of D1.

2.2 D3 discloses the transmission of encrypted information between a fixed network and a mobile station through a base station (see Figure 1: "base control station" and "mobile station"). In the base control station of the fixed network, packets are encrypted using downward radio frame numbers RFNs generated in the base control station (see column 9, lines 10-24). In the base station, the RFNs are read and stored (see column 13, lines 44-48). The radio frame numbers are sent together with the respective encrypted information data via the base station to the mobile station (see column 9, line 10 to column 10, line 51).

3. Inventive step - Article 56 EPC

3.1 Closest prior art

With respect to claim 1 on which the decision was based, present claim 1 contains the additional features that the ciphering of packets is performed in an access gateway and that the output packets are generated at a base station. In D1, both tasks are performed at a base station of a mobile communication network. D3 however relates to the ciphering of packets at a core network entity (see Figure 1: "base control station 21") with full sequence numbers ("radio frame number") for transmission through a base station ("base station 25") to a mobile entity ("mobile station 27"). The board therefore agrees with the appellant that D3 represents the closest prior art because of the structural and functional arrangement disclosed therein.

3.2 The differences between the subject-matter of claim 1 and the disclosure of D3 are thus that the output packets generated by the base station include a partial sequence number used for re-ordering and deciphering

the output packets by the mobile station and that the partial sequence number is derived from the full sequence number.

The technical effect achieved by these distinguishing features is that the full sequence number does not need to be sent to the mobile station and that re-ordering of the packets is possible without ambiguity.

The objective technical problem can thus be formulated as how to improve packet re-ordering at the mobile station, with lower overhead. In that respect, the board does not agree with the appellant that the problem should relate to improving the prevention of packet ambiguity by handover. In the board's view, the packet disambiguity by handover is only one of the consequences of the re-ordering of packets based on the partial sequence numbers.

The skilled person trying to solve this problem would come across document D1, which relates to a wireless communication protocol using ciphering. The skilled person would note that the re-ordering of packets represents an important issue of D1 (see in this respect paragraph [0005], lines 12 to 21). Moreover, the skilled person would realise that the ciphering and packet numbering scheme described in D1 (see section 2.1 above) reduces the overhead by transmitting only part of the encryption key to the mobile station. The skilled person would thus be incited to apply the teaching of D1 in that respect to the system of D3, and output ciphered packets at the base station of D3, including a partial sequence number derived from the full sequence number which was used for encryption, as foreseen by D1 (see section 2.1 above). The skilled

person would arrive in this way at the subject-matter of claim 1.

For these reasons the board judges that the subject-matter of claim 1 does not involve an inventive step (Article 56 EPC), having regard to the combination of D3 and D1.

3.3 The appellant argued that the skilled person would not consider combining D1 with D3 since these documents related to quite different communication systems. In particular, D1 did not relate to communication between a fixed network and a mobile station. In that respect, the appellant referred to Figure 2 of the application which showed that in the alleged invention ciphering/deciphering occured in the PDCP layer present only in the access gateway and in the mobile station, while the numbering/re-ordering of packets occured in the RLC layer present only in the base station and in the mobile station. In D1, no access gateway was involved in the ciphering of packets, whereas in D3 packet numbering involved the gateway. Furthermore, the FN numbers in D1 (see paragraph [0005]) represented frame numbers and not packet numbers and the encryption/decryption of packets took place in the RLC layers of the base and mobile stations (see paragraph [0010]). The appellant further argued that, even if the skilled person combined D3 and D1, he would have to make a selection of features in D1 so that he would not arrive at the subject-matter of claim 1 without the exercise of inventive step.

The board is however not convinced by these arguments, for the following reasons. Claim 1 makes no mention at all of any communication layer, but merely defines in which entity, namely the access gateway, the base

station and the receiving entity, each operation of ciphering input packets, generating output packets, and re-ordering and deciphering the output packets, respectively, are performed. The skilled person would thus not be deterred from consulting D1 by the fact that this document mentions that the RLC layer in both base and mobile stations is used for packet numbering. Further, the features of D1 that the skilled person would implement in D3 are all described in paragraph [0010] of D1, namely that the base station generates output packets including a partial sequence number, i.e. the FN number in the terminology of D1, derived from the full sequence number which was used for encryption, i.e. the count-c value made of the HFN and FN numbers.

Order

For these reasons it is decided that:

The appeal is dismissed.

The Registrar: The Chair:

K. Götz-Wein A. Ritzka

Decision electronically authenticated