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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
27 February 2003 (27.02.2003)

PCT

(10) International Publication Number
WO 03/017568 A1

(51) International Patent Classification[7]: H04L 9/08

(21) International Application Number: PCT/IB02/03429

(22) International Filing Date: 12 August 2002 (12.08.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
0120133.4 17 August 2001 (17.08.2001) GB

(71) Applicant *(for all designated States except US)*: **NOKIA CORPORATION** [FI/FI]; Keilalahdentie 4, FIN-02150 Espoo (FI).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **EDNEY, Jonathan** [GB/GB]; 31 High Street, Willingham, Cambridgeshire CB4 5ES (GB). **BLACK, Simon** [GB/GB]; 66 High Street, Swaffham Prior, Cambridgeshire CB5 0LD (GB).

(74) Agents: **JOHNSON, Ian** et al.; Nokia IPR Department, Nokia House, Summit Avenue, Farnborough, Hampshire GU14 ONG (GB).

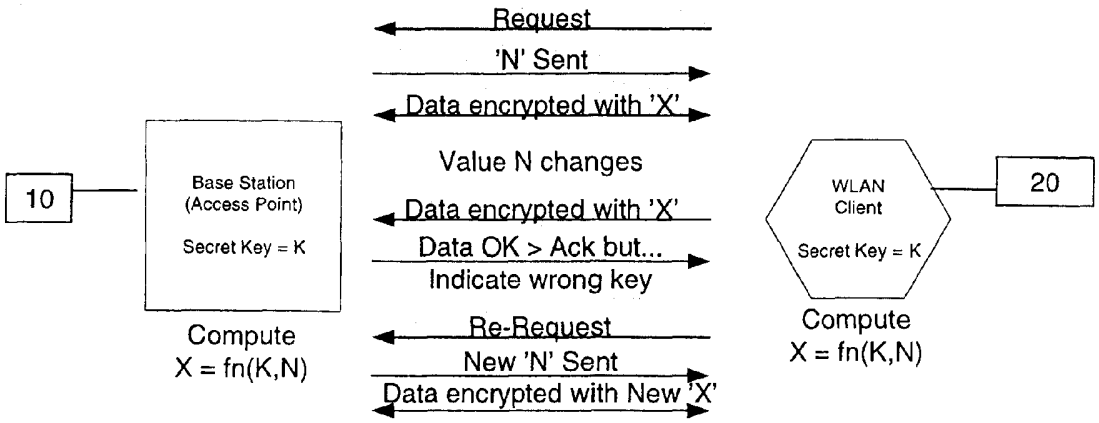
(81) Designated States *(national)*: AE, AG, AL, AM, AT (utility model), AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ (utility model), CZ, DE (utility model), DE, DK (utility model), DK, DM, DZ, EC, EE (utility model), EE, ES, FI (utility model), FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK (utility model), SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: SECURITY IN COMMUNICATIONS NETWORKS



(57) Abstract: The invention provides a method of providing secure data communication between a client device and a network device, wherein the method comprises arranging a periodically varying broadcast code (N) to be transmitted such that the network and client devices have knowledge of the broadcast code (N), providing the network and client devices each with the same secret key code (K) and encryption/decryption algorithm, wherein the algorithm is arranged to encrypt and decipher a encrypted transmission data code used for network authentic data transmissions between the client and network devices, and wherein the encrypted data code is generated from a combination of the data and a secret key (X) which is itself derived from a combination of the secret key code (K) and broadcast code (N). One embodiment provides that the broadcast code (N) is transmitted on request by a network/client device. Another embodiment provides that the ACK frame of a data transmission between client/network devices is used to send notifications of the fact that the broadcast code (N) has changed.

WO 03/017568 A1

Security in Communications Networks

The invention relates to the field of communications networks and aims to increase secure data communications between a client device connected to the network via a network device. In particular, but not exclusively, the invention is applicable to a Wireless Local Area Network (WLAN) which provides wireless data communications between a remote client device and an access point device, and such a situation will be used as an example throughout the specification.

Wireless transmissions are liable to interception and thus WLANs utilise security in the form of encryption. However, encryption methods are subject to "attack" by hackers who monitor transmissions and attempt to break the encryption code. Most of these types of attack rely on capturing large numbers of encrypted messages or massive offline computations to obtain the secret key used for encryption. A simple and effective means of protection against such attacks is to change the secret key frequently so that attackers do not have enough time, or enough messages, to break the code. For example, changing the secret key every five minutes would provide good protection in most networks.

Another proposed solution in the public domain is summarised here as background information, with reference to Figure 1 which is a schematic illustration of the proposed prior art solution. This is the encryption method proposed to be used for IEEE802.11 (WEP).

At a regular interval, such as ten times a second, a 128 bit number (N) is broadcast to all wireless LAN clients (including hackers). The 128 bit number (N) is combined with a secret key (K) known only to the authorised clients and

the access point device. This results in the combination called X and the value of X is used as the encryption key for subsequent transmitted data (Figure 1). Since hackers do not know the value K they cannot compute X and although they can now attempt to discover X, discovery of X does not enable K to be derived due to the complexity of the algorithm combining N and K. This is because, although it is difficult to discover X due to the complexity of the encryption algorithm, it is an important property of the algorithm combining N and K that even if X is discovered by breaking the code, K cannot be extracted from X. Furthermore, as N (and hence X) is changed periodically (say five minute intervals), hackers are not given an opportunity to monitor a sufficient transmission sample in order to be able to break the encryption algorithm. Thus, the secret key K remains secure even if hackers crack the value of X. Nevertheless, severe weaknesses in the encryption method used for IEEE802.11 (WEP) have been discovered and published. There is therefore an imperative to implement rapid secret key updates.

Accordingly, in a first aspect the present invention provides a method of providing secure data communication between a client device and a network device, wherein the method comprises arranging a periodically varying broadcast code (N) to be transmitted such that the network and client devices have knowledge of the broadcast code (N),

providing the network and client devices each with the same secret key code (K) and encryption/decryption algorithm, wherein the algorithm is arranged to encrypt and decipher an encrypted transmission data code used for network authentic data transmissions between the client and network devices, and wherein the encrypted data code is generated from a combination of the data and a secret key (X) which is itself derived from a combination of the secret key code (K) and broadcast code (N),

characterised wherein the broadcast code (N) is transmitted on request by a network/client device.

Although the broadcast code (N) is still transmitted periodically, it is now not transmitted continuously at regular intervals and therefore the method contributes to minimising the transmission of the broadcast code (N). This therefore frees up valuable bandwidth. Accordingly, this invention provides a solution with lower overheads than the current method. This is because overhead, which is the amount of the channel which is used for management related information rather than actual data, is reduced by avoiding the need to send the broadcast code (N) ten times a second. Accordingly, the invention provides a more efficient network which uses less valuable network resources.

A hacker will also find it more difficult to predict when the broadcast code (N) has been changed, as he will not necessarily be able to monitor all changes in broadcast code (N). Therefore the hacker will be less certain of which broadcast code (N) is associated with which particular intercepted encrypted data code transmission, making it increasingly difficult to decipher the transmission. The method also provides continued association of the network and client devices which are still able to communicate using a dynamic encryption data code i.e. one which changes over time due to the changing value of the broadcast code (N). Such a method is also able to handle client/network devices of varying speed, some of which may not necessarily have sufficient speed to efficiently deal with rapid changes in broadcast code (N).

Furthermore, if the method is arranged to identify the particular network/client device by the fact that it is requesting the broadcast code (N), it is possible to provide the broadcast code (N) to the particular device requesting the broadcast code (N). It is further possible to arrange this method to preferably deliver a different value of broadcast code (N) to each network/client device

and/or to change the value of broadcast code (N) at different times for each client device. Such methods of operation are not possible with the prior art arrangement as the prior art methods are not arranged to request the broadcast code (N) and thereby cannot identify the device by the fact that it is requesting the broadcast code (N).

As part of the existing IEEE802.11 standard, a wireless client device is connected to an access point device by sending an "associate request" message, and the access point device replies with an "associate response" if it accepts the client device. "Re-associate request" is a variant whereby a client device, which was previously connected to one access point device, can migrate and be connected to a new access point device. According to one embodiment of this invention, the request for the broadcast code (N) and/or the value of the broadcast code (N) is preferably transmitted as part of an "associate" and/or "re-associate" message exchange. For example, the request for the broadcast code (N) may be sent as part of the "associate request", and the value of the broadcast code (N) could be returned as part of the "associate response".

With the use of associate messaging, it is possible to advantageously transmit the broadcast code (N) to the specific device which requested the code. With the use of associate/re-associate messaging in this manner, the present invention can also be conveniently modified to preferably deliver a different value of broadcast code (N) to each network/client device and/or also to change the value of N at different times for each network/client device.

It would be advantageous to use the ACK frame of a data transmission between client/network devices to send notifications of the fact that the broadcast code (N) has changed. The ACK frame is currently used to acknowledge receipt of a transmission and therefore the invention would

provide supplementary use for the ACK frame. Furthermore, the method can advantageously be implemented using existing hardware by incorporating a software change to the network/client device. In the case of the IEEE802.11 standard for example, the ACK frame has spare capacity which can conveniently be used by the present invention.

With the use of the ACK frame in this manner, the present invention can be conveniently modified to preferably provide a notification for each different value of broadcast code (N) to each network/client device and/or also for each change of the value of broadcast code (N) with time for each network/client device.

Although the ACK frame, or more specifically the WEP bit of an ACK frame, could be used to send a request to transmit the broadcast code (N), it would be convenient to use the above mentioned associate/re-associate message exchange.

In a preferred embodiment, the method provides a transition phase where it is checked whether the encrypted data code was generated using a secret key (X) derived from a current or recent broadcast code (N), and in the case of the secret key (X) being generated using a recent broadcast code (N), the appropriate client/network device is notified it is not using the current broadcast code (N) such that the appropriate client/network device subsequently requests the current broadcast code (N).

This method has the advantage that it is possible to keep track of which network/client devices have updated their encryption keys.

To send the notification that the current broadcast code (N) is not being used, it would be convenient to again use a bit in the ACK frame of a data

transmission, but in this case, the ACK frame would be one which is sent in response to a received data transmission generated using the recent (i.e. the non-current) broadcast code (N). In a IEEE802.11 standard communications network, it would be particularly advantageous to use the "WEP" bit which is not used by the ACK frame in current systems.

Preferably, this invention proposes that the network/client device would re-associate to the same device in order to get the new value of broadcast code (N) after being notified of a change in broadcast code (N).

In a second aspect, the present invention provides a method of providing secure data communication between a client device and a network device, wherein the method comprises arranging a periodically varying broadcast code (N) to be transmitted such that the network and client devices have knowledge of the broadcast code (N),

providing the network and client devices each with the same secret key code (K) and encryption/decryption algorithm, wherein the algorithm is arranged to encrypt and decipher a encrypted transmission data code used for network authentic data transmissions between the client and network devices, and wherein the encrypted data code is generated from a combination of the data and a secret key (X) which is itself derived from a combination of the secret key code (K) and broadcast code (N),

characterised wherein the ACK frame of a data transmission between client/network devices is used to send notifications of the fact that the broadcast code (N) has changed.

The ACK frame is currently used to acknowledge receipt of a transmission and therefore this aspect of the invention would provide supplementary use for the ACK frame. Furthermore, the method can advantageously be implemented using existing hardware by incorporating a software change to

the network/client device. In the case of the IEEE802.11 standard for example, the ACK frame has spare capacity which can conveniently be used by the present invention.

In one embodiment, the broadcast code (N) is transmitted on request by a network/client device. Preferably, the request for the broadcast code (N) is transmitted as part of an "associate" and/or "re-associate" message exchange. Specifically, the request for the broadcast code (N) may be transmitted as part of the "associate request".

Preferably, the value of the broadcast code (N) is transmitted as part of an "associate" and/or "re-associate" message exchange. Specifically, the value of the broadcast code (N) is returned as part of the "associate response".

Similarly to the modified method according to the first aspect of the invention, the method according to the second aspect of the invention may be arranged to deliver a different value of broadcast code (N) to each network/client device. Furthermore, the method may be arranged to change the value of the broadcast code (N) at different times for each network/client device.

To make it more difficult to predict when the broadcast code (N) has been changed, the methods may preferably vary the frequency at which the broadcast code (N) is changed.

The broadcast code (N) may be transmitted on request by a network/client device which is recognised by the network e.g. by analysing the appropriate MAC number or by password authentication. However, the broadcast code (N) is preferably transmitted on request by a network/client device using a network authentic encryption data code (X). These two methods may be used in combination. For example, it may be that on initial sign on of the client and

network devices, the client/network device may not have the current broadcast code (N) and therefore may not be using the current encryption data code. In this case, the transmission will not be recognised as a network authentic data code and the broadcast code (N) would be transmitted on request by a network/client device which is recognised by the network. However, the method may be limited to the transmission of the broadcast code (N) only on request by a network/client device using a network authentic encryption data code.

Preferably, the broadcast code (N) itself may be encrypted by a separate or the same encryption algorithm, thereby making it more difficult for a hacker to decipher the encryption data code.

Although the methods may advantageously be applied to wireless communications between a client device and a network device, it may equally be applied to wired communications between client/network devices. However, the invention is thought to have particular advantages if applied to a WLAN network or a Bluetooth™ network.

The methods may be modified such that the broadcast code (N) is transmitted by either the network device, or by a device independent of the network device, which in unusual circumstances may be a client device. The method encompasses embodiments wherein either one, or both, of the transmissions from the client/network device are encrypted.

The invention also encompasses network and/or client devices configured to operate in all of the above-mentioned manners.

Specific embodiments of the present invention will now be described by way of example only with reference to the following figures in which :

Figure 1 is a schematic representation of a prior art solution to providing security in a WLAN;

Figure 2 is a schematic representation of data communications according to one embodiment of the present invention.

The proposed invention relates to a refinement to the prior art method described above. The current proposed prior art method is inefficient because the value N is broadcast frequently, wasting valuable bandwidth. One embodiment of the present proposal is that the value of N is only sent when requested by the client.

As part of the existing IEEE802.11 standard, a wireless client device 20 is connected to an access point device 10 by sending an "associate request" message, and the access point device 10 replies with an "associate response" if it accepts the client device 20. "Re-associate request" is a variant whereby a client device 20, which was previously connected to one access point device 10, can migrate and be connected to a new access point device 10. According to this embodiment, the value of broadcast code (N) would be requested and delivered as part of the associate/re-associate message exchange.

A further problem to be solved is how to notify the client device 20 that the value of N has changed and how to maintain communications while the new value of X is computed. The invention proposes that there would be a key transition phase (say one minute) during which time the client device 20 could use either the old or the new value of X for encryption. The key choice (old or new) would be indicated in the frame (using existing key ID bits for IEEE802.11 which have been designed to identify which secret key X was used to encrypt the transmission).

During the transition phase, the access point device 10 will detect if the client device 20 uses the old value of X. It will accept and decrypt the message but will notify the client in the manner described below, and illustrated schematically in Figure 2. Once the client device 20 is notified that it is using an out-of-date key it can initiate an exchange to obtain the new value of X.

Notification of the client device 20 is provided using a bit in the ACK frame which is typically sent in response to data frame. In the case of IEEE802.11, the ACK frame has an existing bit "WEP" which is unused and would be appropriate to this purpose. This has the advantage that the method could be applied for existing systems using only firmware upgrades.

This embodiment is arranged such that the client device 20 would re-associate to the same access point device 10 in order to get the new value of (N) after being notified of a change. However, other embodiments may allow re-association to a different access point device 10.

Claims

1. A method of providing secure data communication between a client device and a network device, wherein the method comprises arranging a periodically varying broadcast code (N) to be transmitted such that the network and client devices have knowledge of the broadcast code (N),

providing the network and client devices each with the same secret key code (K) and encryption/decryption algorithm, wherein the algorithm is arranged to encrypt and decipher an encrypted transmission data code used for network authentic data transmissions between the client and network devices, and wherein the encrypted data code is generated from a combination of the data and a secret key (X) which is itself derived from a combination of the secret key code (K) and broadcast code (N).

2. The method according to claim 1, wherein the broadcast code (N) is transmitted on request by a network/client device.

3. The method according to claim 2, comprising identifying the particular network/client device by the fact that it is requesting the broadcast code (N) and arranging to provide the broadcast code (N) to the particular device requesting the broadcast code (N).

4. The method as claimed in claim 3, comprising arranging to deliver a different value of broadcast code (N) to each network/client device.

5. The method of claim 3 or claim 4, comprising arranging to deliver a different value of broadcast code (N) to a network/client device at different times.

6. The method of any of the preceding claims, wherein the request for the broadcast code (N) is transmitted as part of an “associate” and/or “re-associate” message exchange.

7. The method as claimed in claim 6, wherein the request for the broadcast code (N) is transmitted as part of the "associate request".

8. The method of any of the preceding claims, wherein the value of the broadcast code (N) is transmitted as part of an “associate” and/or “re-associate” message exchange.

9. The method as claimed in claim 8, wherein the value of the broadcast code (N) is returned as part of the "associate response".

10. The method as claimed in any of claims 6 to 9, wherein the method is arranged to deliver a different value of broadcast code (N) to each network/client device.

11. The method as claimed in any of claims 6 to 10, wherein the method is arranged to change the value of the broadcast code (N) at different times for each network/client device.

12. The method as claimed in any of the preceding claims, wherein a notification of the fact that the broadcast code (N) has changed is transmitted by the use of the ACK frame.

13. The method as claimed in claim 12, wherein the WEP bit of the ACK frame is used to send the notification.

14. The method as claimed in any of the preceding claims, wherein the method provides a transition phase where it is checked whether the encrypted data code was generated using a secret key (X) derived from a current or recent broadcast code (N), and in the case of the secret key (X) being generated using a recent broadcast code (N), the appropriate client/network device is notified it is not using the current broadcast code (N) such that the appropriate client/network device subsequently requests the current broadcast code (N).

15. The method as claimed in claim 14, wherein the ACK frame is used to send the notification that the current broadcast code (N) is not being used.

16. The method as claimed in claim 15, wherein the WEP bit in the ACK frame is used to send the notification.

17. The method as claimed in claims 14-16, wherein the network/client device re-associates to the same device in order to get the new value of broadcast code (N) after being notified of a change in broadcast code (N).

18. The method according to any preceding claim, wherein the ACK frame of a data transmission between client/network devices is used to send notifications of the fact that the broadcast code (N) has changed.

19. The method as claimed in claim 18, wherein the WEP bit of the ACK frame is used to send the notification.

20. The method as claimed in 18 or claim 19, wherein the broadcast code (N) is transmitted on request by a network/client device.

21. The method as claimed in claims 18-20, wherein the request for the broadcast code (N) is transmitted as part of an “associate” and/or “re-associate” message exchange.

22. The method as claimed in claim 21, wherein the request for the broadcast code (N) is transmitted as part of the "associate request".

23. The method as claimed in claims 18-22, wherein the value of the broadcast code (N) is transmitted as part of an “associate” and/or “re-associate” message exchange.

24. The method as claimed in claim 23, wherein the value of the broadcast code (N) is returned as part of the "associate response".

25. The method as claimed in claims 18-24, wherein the method is arranged to deliver a different value of broadcast code (N) to each network/client device.

26. The method as claimed in claims 18-25, wherein the method is arranged to change the value of the broadcast code (N) at different times for each network/client device.

27. The method as claimed in claims 18-26, wherein the method provides a transition phase where it is checked whether the encrypted data code was generated using a secret key (X) derived from a current or recent broadcast code (N), and in the case of the secret key (X) being generated using a recent broadcast code (N), the appropriate client/network device is notified it is not using the current broadcast code (N) such that the appropriate client/network device subsequently requests the current broadcast code (N).

28. The method as claimed in any of the preceding claims, wherein the frequency at which the broadcast code (N) is changed is varied.

29. The method as claimed in any of the preceding claims, wherein the broadcast code (N) is transmitted on request by a network/client device which is recognised by the network.

30. The method as claimed in any of the preceding claims, wherein the broadcast code (N) is transmitted on request by a network/client device using a network authentic encryption data code (X).

31. The method as claimed in claim 29 or claim 30, wherein the transmission of the broadcast code (N) is only on request by a network/client device using a network authentic encryption data code.

32. The method as claimed in any of the preceding claims, wherein the broadcast code (N) itself is encrypted by a separate or the same encryption algorithm.

33 The method according to any of the preceding claims applied to wireless communications between a client device and a network device.

34. A client/network device arranged to operate according to any of the preceding methods.

35. A method as hereinbefore described and with reference to the accompanying drawings.

36. A client/network device as hereinbefore described and with reference to the accompanying drawings.

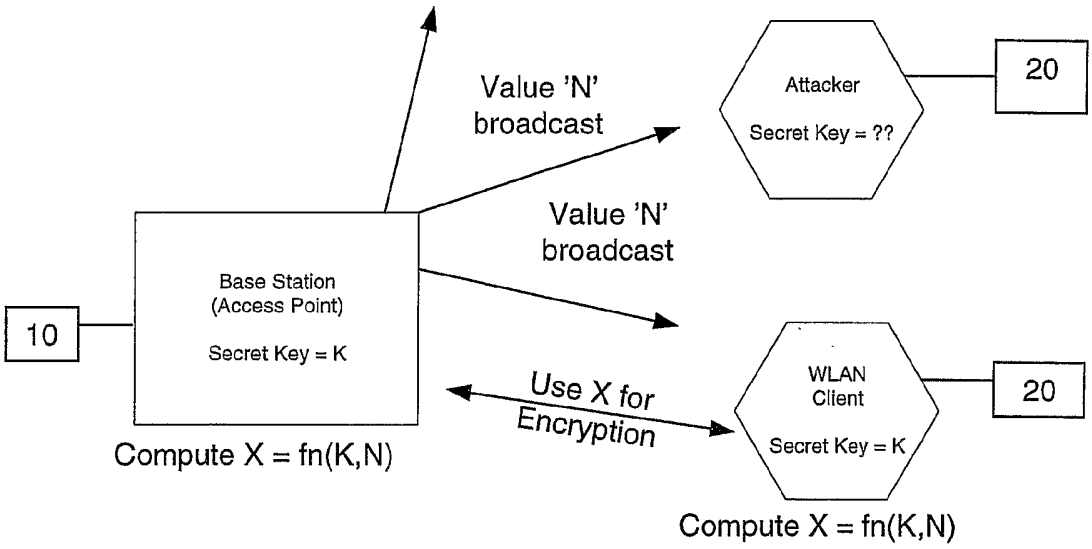


Figure 1

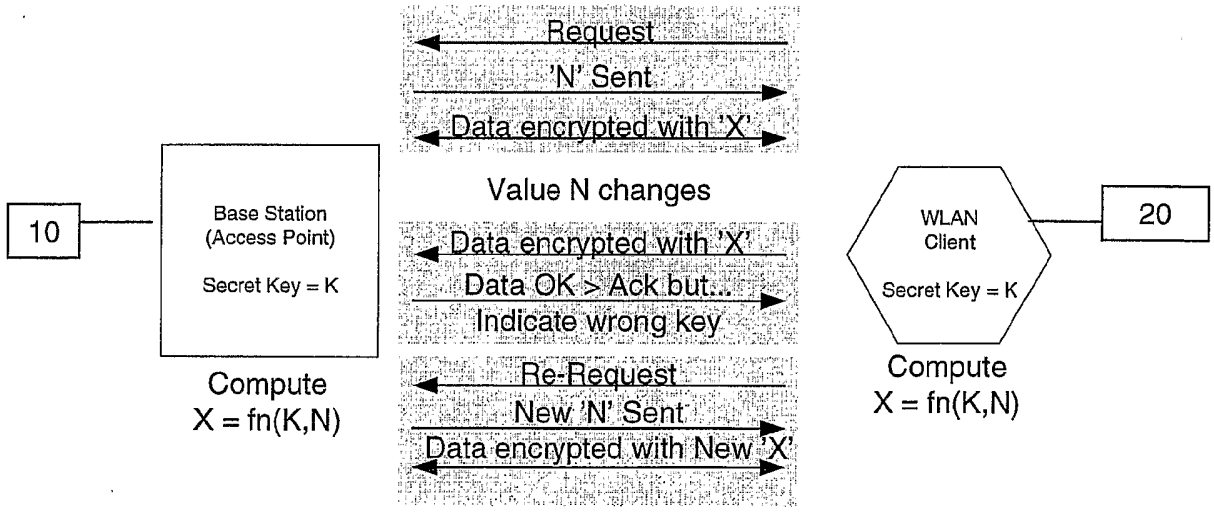


Figure 2

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IB 02/03429

A. CLASSIFICATION OF SUBJECT MATTER

IPC7: H04L 9/08
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC7: H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-INTERNAL, WPI DATA

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 1098471 A2 (PITNEY BOWES INC.), 9 May 2001 (09.05.01), abstract --	1-36
A	US 5889861 A (OHASHI, M. ET AL), 30 March 1999 (30.03.99), abstract --	1-36
A	US 5963646 A (FIELDER, G.L. ET AL), 5 October 1999 (05.10.99), abstract --	1-36
A	US 6088799 A (MORGAN, S.P. ET AL), 11 July 2000 (11.07.00), abstract --	1-36

[X] Further documents are listed in the continuation of Box C. [X] See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
26 November 2002	29-11-2002
Name and mailing address of the ISA/ Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86	Authorized officer Rune Bengtsson /OGU Telephone No. +46 8 782 25 00

Form PCT/ISA/210 (second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IB 02/03429

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
P,A	WO 0233884 A2 (SUN MICROSYSTEMS, INC.), 25 April 2002 (25.04.02), the whole document -- --------	1-36

INTERNATIONAL SEARCH REPORT

Information on patent family members

28/10/02

International application No.
PCT/IB 02/03429

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 1098471 A2	09/05/01	NONE	
US 5889861 A	30/03/99	GB 2297016 A,B	17/07/96
		GB 9525817 D	00/00/00
		JP 3271460 B	02/04/02
		JP 8195741 A	30/07/96
US 5963646 A	05/10/99	EP 0966810 A	29/12/99
		JP 2001514834 T	11/09/01
		US 6105133 A	15/08/00
		WO 9845980 A	15/10/98
US 6088799 A	11/07/00	NONE	
WO 0233884 A2	25/04/02	AU 1328402 A	29/04/02