

(19) World Intellectual Property
Organization
International Bureau



(43) International Publication Date
29 January 2004 (29.01.2004)

PCT

(10) International Publication Number
WO 2004/010636 A1

(51) International Patent Classification⁷: **H04L 9/00**

(21) International Application Number:
PCT/US2003/020470

(22) International Filing Date: 27 June 2003 (27.06.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
10/197,148 17 July 2002 (17.07.2002) US

(71) Applicant: **HARRIS CORPORATION** [US/US]; 1025
W. NASA Blvd., Melbourne, FL 32919 (US).

(72) Inventor: **BILLHARTZ, Thomas, Jay**; 2355 Polonius
Lane, Melbourne, FL 32934 (US).

(74) Agents: **YATSKO, Michael, S.** et al.; Harris Corporation,
1025 W. NASA Blvd., Melbourne, FL 32919 (AU).

(81) Designated States (*national*): AE, AG, AL, AM, AT, AU,
AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU,
CZ, DE, DK, DM, DZ, EC, EE, ES, 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,
SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VN, YU,
ZA, ZM, ZW.

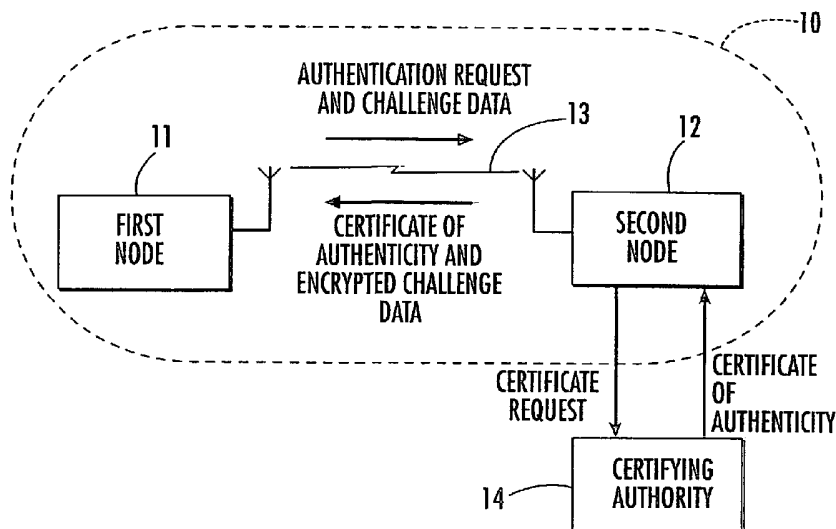
(84) Designated States (*regional*): ARIPO patent (GH, GM,
KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW),
Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM),
European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE,
ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO,
SE, SI, SK, TR), OAPI patent (BF, BJ, 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: MOBILE AD-HOC NETWORK INCLUDING NODE AUTHENTICATION FEATURES AND RELATED METHODS



(57) **Abstract:** A mobile ad-hoc network may include a first node having a first public key and a first private key associated therewith for generating an authentication request. The network may also include a second node having a second public key and a second private key associated therewith for receiving the authentication request and returning a certificate of authenticity including the second public key to the first node. Upon verifying that the second public key belongs to the second node, the first node may send challenge data to the second node, and the second node may encrypt the challenge data using the second private key and return the encrypted challenge data back to the first node. The first node may thus decrypt the encrypted challenge data using the verified second public key and authenticate the second node if the decryption of the encrypted challenge data yields the original challenge data.

**MOBILE AD-HOC NETWORK INCLUDING NODE
AUTHENTICATION FEATURES AND RELATED METHODS**

Field of the Invention

The present invention relates to the field of communications, and, more particularly, to mobile ad-hoc networks and related methods.

5

Background of the Invention

Wireless networks have experienced increased development in the past decade. One of the most rapidly developing areas is mobile ad-hoc networks. Physically, a mobile ad-hoc network includes a number of geographically-distributed, potentially mobile nodes sharing a common radio channel. Compared with other types of networks, such as cellular networks or satellite networks, the most distinctive feature of mobile ad-hoc networks is the lack of any fixed infrastructure. The network may be formed of mobile nodes only, and a network is created "on the fly" as the nodes come close enough to transmit with each other. The network does not depend on a particular node and dynamically adjusts as some nodes join or others leave the network.

Because of these unique characteristics, routing protocols for governing data flow within ad-hoc networks are required which can adapt to frequent topology changes. Two basic categories of ad-hoc routing protocols have emerged in recent years, namely reactive or "on-demand" protocols, and proactive or table-driven protocols. Reactive protocols collect routing information when a particular route is required to a destination in response to a route request. Examples of reactive protocols include ad-hoc on demand distance vector (AODV) routing, dynamic source routing (DSR), and the temporally ordered routing algorithm (TORA).

On the other hand, proactive routing protocols attempt to maintain consistent, up-to-date routing information from each node to every other node in the network. Such protocols typically require each node to
5 maintain one or more tables to store routing information, and they respond to changes in network topology by propagating updates throughout the network to maintain a consistent view of the network. Examples of such proactive routing protocols include destination-sequenced distance-vector (DSDV) routing,
10 which is disclosed in U.S. Patent No. 5,412,654 to Perkins; the wireless routing protocol (WRP); and clusterhead gateway switch routing (CGSR). A hybrid protocol which uses both proactive and reactive approaches is the zone routing protocol (ZRP), which is disclosed in U.S. Patent No.
15 6,304,556 to Haas.

One challenge to the advancement of ad-hoc network development is that of security. In particular, since nodes are continuously entering and exiting a mobile ad-hoc network the task of ensuring that a node is a trustworthy source for
20 data exchange can be difficult. Because of the early stage of development of ad-hoc networks and the numerous other challenges these networks present, the above routing protocols have heretofore primarily focused solely on the mechanics of data routing and not on such node
25 authentication.

Some approaches are now being developed for performing node authentication within mobile ad-hoc networks. One such approach is outlined in a Capstone Proceeding paper by Nguyen et al. entitled "Security Routing Analysis for
30 Mobile Ad Hoc Networks," Department of Interdisciplinary Telecommunications, University Of Colorado at Boulder, Spring 2000. In this paper, the authors suggest using the U.S. Data Encryption Standard (DES) for encrypting plain text messages. For authentication, digital signatures and keyed one-way

hashing functions with windowed sequence numbers are proposed.

More particularly, public-key encryption is used along with a one-way hash function to provide the digital signature. The sender uses the one-way hash function on the message and then encrypts the hash value with their private key. The message, along with the encrypted hash value, is sent to its destination. At the receiver, the hash value is also calculated based upon the message and is compared with the received hash value that was decrypted with the sender's public key. If they are the same, then the signature is authenticated.

Furthermore, rather than using a centralized (i.e., single) key management authority, a distributed public key management approach is suggested wherein a set of "trustworthy" nodes are designated that share sections of the public key management system. Each trusted node keeps a record of all public keys in the network, and the number of nodes needed to generate a valid signature is less than the total number of trusted nodes.

Another similar public/private key approach is discussed in an article by Zhou et al. entitled "Securing Ad Hoc Networks," IEEE Network Magazine, vol. 13, no.6, November/December 1999. This approach provides for a key management service which, as a whole, has a public/private key pair. All nodes in the system know the public key of the management service and trust any certificates signed using the corresponding private key. Nodes, as clients, can submit query requests to get other clients' public keys or submit update requests to change their own public keys. Internally, the key management service includes n special nodes called servers present within the ad-hoc network. Each server also has its own key pair and stores the public keys of all the nodes in the network. In particular, each server knows the

public keys of other servers. Thus, the servers can establish secure links among themselves.

While the above papers address some aspects of implementing public/private key encryption and authentication in mobile ad-hoc networks, there are still further issues that remain to be addressed. For example, a would-be hacker could surreptitiously pose as an existing node in the network and lure a sending node to mistakenly send data thereto. Unless certain measures are taken, the hacker could act as a "man-in-the-middle" and forward authentication messages (and responses) to the intended destination. As a result, messages could still be altered and/or discarded, potentially crippling network communication.

15 Summary of the Invention

In view of the foregoing background, it is therefore an object of the present invention to provide a mobile ad-hoc network with node authentication features and related methods.

20 This and other objects, features, and advantages in accordance with the present invention are provided by a mobile ad-hoc network which may include a first node for generating an authentication request which has a first public key and a first private key associated therewith. The network may also include a second node having a second public key and a second private key associated therewith. The first node may receive a certificate of authenticity responsive to the authentication request generated by a certifying authority and including the second public key. The certifying authority may have a public authentication key and a private authentication key associated therewith and generate the certificate of authenticity using the private authentication key.

In addition, the first node may decrypt the certificate of authenticity using the public authentication key and verify that the second public key belongs to the second node based upon the decrypted certificate of authenticity. Also, the first node may send challenge data (e.g., random challenge data) to the second node upon verification that the second public key belongs to the second node. Thus, the second node may encrypt the challenge data using the second private key and return the encrypted challenge data back to the first node. As such, the first node may decrypt the encrypted challenge data using the verified second public key and authenticate the second node if the decryption of the encrypted challenge data yields the original challenge data. Accordingly, the first node can therefore advantageously verify that it is indeed communicating with the second node, which has been verified by the certifying authority.

More particularly, the certificate of authenticity may further include a node identification (ID) of the second node. As such, the first node may verify the second public key belongs to the second node by processing the second node ID and the second public key to create a digest, and comparing the digest with the decrypted certificate of authenticity to verify that the second public key belongs to the second node. By way of example, the first node may process the second node ID and the second public key using a hashing algorithm.

Additionally, the first node may, upon authenticating the second node, send a session key to the second node that is encrypted with the second public key for use with subsequent data transfers therebetween. The session key may be a random session key, for example. The use of the session key advantageously reduces the likelihood of an unauthorized man in the middle from being able to interfere

message data sent between the first and second nodes. That is, only the true second node will be able to decrypt the session key that will be used for sending message data between the first and second nodes.

5 Further, the first node may also terminate the authentication of the second node after a predetermined period so that the authentication is kept current. The certificate of authenticity may also include a time of authentication by the certifying authority, for example. In
10 addition, the first and second nodes may communicate using the direct source routing (DSR) protocol, and they may also transfer message data therebetween upon authentication of the second node by the first node. Also, the first node may send the authentication request to the second node, and the second
15 node may return the certificate of authenticity to the first node responsive thereto. In other embodiments, the first node may send the authentication request to the certifying authority and receive the authentication request therefrom.

 A node authentication method aspect of the
20 invention is for a mobile ad-hoc network including a plurality of nodes. The method may include generating an authentication request at a first node having a first public key and a first private key associated therewith to authenticate a second node having a second public key and a
25 second private key associated therewith. Responsive to the authentication request, the first node may receive a certificate of authenticity generated by a certifying authority and including the second public key. The certifying authority may have a public authentication key and
30 a private authentication key associated therewith and generate the certificate of authenticity using the private authentication key

 The method may further include decrypting the certificate of authenticity at the first node using the

public authentication key and verifying that the second public key belongs to the second node based upon the decrypted certificate of authenticity. In addition, challenge data may be sent from the first node to the second node upon verification that the second public key belongs to the second node. The challenge data may be encrypted at the second node using the second private key, and the encrypted challenge data returned back to the first node. Also, the method may further include decrypting the encrypted challenge data at the first node using the verified second public key and authenticating the second node if the decryption of the encrypted challenge data yields the original challenge data.

Brief Description of the Drawings

FIG. 1 is schematic block diagram of a mobile ad-hoc network in accordance with the present invention.

FIGS. 2-7 are more detailed schematic block diagrams of the first and second nodes of the mobile ad-hoc network of FIG. 1 and further illustrating the process of node authentication therebetween in accordance with the present invention.

FIG. 8 is a schematic block diagram of an alternate embodiment of the mobile ad-hoc network of FIG. 1.

FIG. 9 is a flow diagram illustrating a mobile ad-hoc network node authentication method in accordance with the present invention.

Detailed Description of the Preferred Embodiments

The present invention will now be described more fully hereinafter with reference to the accompanying drawings, in which preferred embodiments of the invention are shown. This invention may, however, be embodied in many different forms and should not be construed as limited to the embodiments set forth herein. Rather, these embodiments are

provided so that this disclosure will be thorough and complete, and will fully convey the scope of the invention to those skilled in the art. Like numbers refer to like elements throughout, and prime notation is used to indicate
5 similar elements in alternate embodiments.

Referring initially to FIGS. 1-7, a mobile ad-hoc network **10** in accordance with the invention illustratively includes a first node **11** and a second node **12**. While only the first and second nodes **11**, **12** are shown for clarity of
10 illustration, it will be understood by those of skill in the art that any number of nodes may be included within the mobile ad-hoc network **10**. Fixed nodes may also be included in the mobile ad-hoc network **10** in some embodiments to provide a bridge between the network and a communications
15 infrastructure (e.g., a telephone or cellular network), as will also be understood by those of skill in the art. Of course, such fixed nodes are not required.

In the illustrated example, the first node **11** is an authenticating node in that it is attempting to establish
20 the authenticity or trustworthiness of the second, unauthenticated node **12**. The second node **12** may be unauthenticated, for example, because it recently entered the network **10**, either by being powered on or by coming in range of the network. As noted above, mistakenly sending messages
25 to an unauthenticated node could result in tampering, lost messages, or worse. Thus, in accordance with the invention, the first node **11** will preferably seek to establish the authenticity of the second node **12** (as well as other unauthenticated nodes) before sending message data thereto.

30 To establish the authenticity of the second node **12**, the first node **11** generates an authentication request which it sends to the second node (FIG. 2). As illustratively shown, the first node **11** includes a wireless communications device **21** and a controller **22** that cooperates

with the wireless communications device to establish a wireless communications link **13** to the second node **12**, as will be appreciated by those of skill in the art. The second node **12** similarly includes a wireless communications device
5 **23** and a controller **24**.

By way of example, the first and second nodes **11**, **12** may be laptop computers, personal data assistants (PDAs), or any other devices suitable for use in mobile ad-hoc networks, as will be appreciated by those of skill in the
10 art. As such, the wireless communications devices **21**, **23** may be wireless modems, cellular devices, etc., and the controllers **22**, **24** may be microprocessors, for example.

In accordance with the invention, node authentication is based upon public/private key encryption.
15 More particularly, the first node **11** has a first public key and a first private key associated therewith, and the second node **12** has a second public key and a second private key associated therewith, as will be appreciated by those of skill in the art. Upon receiving the authentication request
20 from the first node **11**, the second node **12** returns a certificate of authenticity to the first node, as illustratively shown in FIG. 3.

The certificate of authenticity is generated by a certifying authority **14** and may be provided to the second
25 node **12** upon request, as illustratively shown in FIG. 1. Preferably, this would be done when the second node **12** enters the network **10**, and it could be updated at certain intervals thereafter. Of course, the second node **12** could request the certificate of authenticity upon receiving the authentication
30 request from the first node **11**, but this will increase the time required for the first node to authenticate the second node and may therefore not be desirable in certain applications.

As briefly described above, in typical prior art approaches using public and private key encryption (such as in Internet security applications, for example), a certifying authority is established as a trusted source from which users
5 can obtain public keys for other users with which they wish to communicate. In accordance with the invention, the certifying authority **14** preferably generates a certificate of authentication for the second node **12** which includes the second public key and a node identification (ID) of the
10 second node.

In particular, the certifying authority **14** has its own public authentication key and private authentication key associated therewith, and it generates the certificate of authenticity using the private authentication key to encrypt
15 the second public key and second node ID. The certifying authority **14** may be a single node in the network **10**, or a plurality of nodes may share this responsibility as proposed in the above papers by Nguyen et al. and Zhou et al., both of which are hereby incorporated herein in their entireties by
20 reference.

Another approach to providing the certifying authority **14** is to group nodes in the network **10** into clusters each having a designated cluster leader node, as described in co-pending U.S. patent application number
25 10/134,559, filed April 29, 2002, and assigned to the Harris Corporation, assignee of the present application, which is hereby incorporated herein in its entirety by reference. Thus, the certifying authority responsibility could be distributed to the cluster leader nodes, as will be
30 appreciated by those of skill in the art.

Upon receiving the certificate of authenticity (FIG. 3), the first node **11** decrypts the certificate of authenticity using the public authentication key of the certifying authority **14**, which is generally known by all of

the nodes in the network **10**. This is done to verify that the second public key belongs to the second node **12**. More particularly, the first node **11** verifies the second public key belongs to the second node **12** by processing the second
5 node ID and the second public key to create a digest. By way of example, the first node **11** may process the second node ID and the second public key using a hashing algorithm to create the digest. The digest may then be compared with a digest of the decrypted certificate of authenticity to verify that the
10 second public key belongs to the second node **12**, as will be understood by those of skill in the art.

By performing the foregoing steps, the first node **11** is able to verify that it is communicating with a node that has a certificate of authenticity from a trustworthy
15 source (i.e., the certifying authority **14**), and that it has the correct second public key for the second node **12**. Yet, at this point it is still possible that the information the first node **11** is receiving is not from the true node **12**. That is, a would-be hacker posing as the second node **12** could
20 have previously intercepted the certificate of authenticity and provided this certificate to the first node **11** in response to the authentication request. As such, typical prior art public/private key encryption approaches, such as those noted above, which rely solely upon a certificate of
25 authenticity could still be susceptible to compromise.

In accordance with the present invention, the first node **11** preferably sends challenge data to the second node **12** upon verification that the second public key belongs to the second node (FIG. 4). The second node **12** will then
30 encrypt the challenge data using the second private key and return the encrypted challenge data back to the first node **11** (FIG. 5). By way of example, the challenge data may be randomly generated to provide yet additional security, as

will be appreciated by those of skill in the art. Of course, other types of challenge data may also be used.

Accordingly, the first node **11** decrypts the encrypted challenge data using the previously verified second public key and authenticates the second node **12** if the decryption of the encrypted challenge data yields the original challenge data. The first node **11** can therefore advantageously verify that it is indeed communicating with the second node **12**, and it has already been established that the second node has been verified by the certifying authority **14**. The only remaining security breach to guard against at this point is that of a man in the middle intercepting and potentially repeating or otherwise tampering with messages, for example.

To reduce the likelihood of such an occurrence, in some embodiments the first node **11** also sends a session key to the second node **12** that is encrypted with the second public key (FIG. 6). Because it is encrypted with the second public key, only the second node (which has the second private key) can decrypt and determine the session key. This session key may then be used for subsequent data transfers between the first and second nodes **11**, **12** to provide symmetric data encryption.

As such, the use of the session key advantageously reduces the likelihood of an unauthorized man in the middle from being able to intercept and decrypt message data sent between the first and second nodes **11**, **12**. That is, only the true second node **12** will be able to decrypt the session key that will be used for sending message data between the first node **11** and the second node. The session key may be a random session key, for example, but here again any suitable type (or size) of session key known to those of skill in the art may also be used.

In some embodiments, the first node **11** preferably terminates the authentication of the second node after a predetermined period so that the authentication is kept current. Similarly, the certificate of authenticity may also include a time of authentication (which may include the date) by the certifying authority **14**, for example. Here again, this is another approach to keep the authentication current, which can be extremely important in the mobile ad-hoc network context where nodes are continuously entering and exiting the network.

Other information that may be included in the certificate of authenticity in other embodiments include a media access layer (MAC) address, an Internet Protocol (IP) address, and/or a personal computer (PC) identification. Of course, one or more of the above security measures and/or types of certificate information may be used in various embodiments depending upon the level of security and network performance required, as will be understood by those of skill in the art.

Once the second node **12** has been properly authenticated and, optionally, the session key distributed thereto, the first node **11** and the second node may transfer message data therebetween in accordance with the given mobile-ad hoc protocol begin used (FIG. 7). As used herein, "message data" is intended to include any data that may be sent between nodes in a mobile ad-hoc network during normal operation, including (but not limited to) route requests/replies, video data, audio data, alphanumeric data, etc. By way of example, if the present invention is implemented with the direct source routing (DSR) protocol, then the first node **11** would preferably only authenticate the second node **12** and leave any downstream authentication to the downstream nodes. Stated alternately, once the first node **11** establishes the trustworthiness of the second node **12**, it

would rely on the second node **12** to authenticate the next node along a route, and so on until all of the nodes along a particular route were authenticated. Of course, those of skill in the art will appreciate that the present invention
5 may be implemented with other suitable mobile ad-hoc network protocols as well, such as those previously noted above, for example.

In the above-described example, the first node **11** sends the authentication request to the second node **12** and
10 the second node returns the certificate to the first node. In such case, the second node **11** will have previously obtained the certificate of authenticity from the certifying authority **14** or it will do so responsive to the authentication request. In the alternate embodiment
15 illustrated in FIG. 8, the first node **11'** sends the authentication request to the certifying authority **14'** and receives the certificate of authenticity directly therefrom, as will be appreciated by those of skill in the art. Furthermore, the second node **12'** may similarly authenticate
20 the first node **11'** prior to message data being sent therebetween. That is, a two-way authentication may be used in certain embodiments, if desired. The remaining elements illustrated in FIG. 8 are similar to those previously noted above and will therefore not be discussed further herein.

25 A node authentication method aspect of the invention for the mobile ad-hoc network **10** is now described with reference to FIG. 9. The method begins (Block **90**) by generating an authentication request at first node **12** having a first public key and a first private key associated
30 therewith, and sending the authentication request from the first node to a second node **12** having a second public key and a second private key associated therewith, at Block **91**. Further, a certificate of authenticity is returned from the second node **12** to the first node **11**, at Block **92**.

The certificate of authenticity is preferably generated by the certifying authority **14** and include the second public key, as noted above. Again, the certifying authority has a public authentication key and a private authentication key associated therewith and generates the certificate of authenticity using the private authentication key. Of course, in some embodiments the certificate of authenticity may be obtained directly from the certifying authority by the first node **11**, as previously discussed above.

The method may further include decrypting the certificate of authenticity at the first node **11** using the public authentication key, at Block **93**, and verifying that the second public key belongs to the second node **12** based upon the decrypted certificate of authenticity, at Block **94**. If it does not, the first node will abort the authentication process (Block **100**) and will not authenticate the second node **12**. As such, no message data will be sent to the second node **12**, thus concluding the method (Block **102**). On the other hand, if it is verified that the second public key indeed belongs to the second node **12**, challenge data is sent from the first node **11** to the second node, at Block **95**. The challenge data is then encrypted at the second node **12** using the second private key, and the encrypted challenge data returned back to the first node, at Block **96**.

Also, the method further includes decrypting the encrypted challenge data at the first node **11** using the verified second public key, at Block **97**. If the decryption of the encrypted challenge data yields the original challenge data (Block **98**), as described above, then the second node **12** is authenticated by the first node **11**, at Block **99**, and the transfer of message data therebetween may begin (Block **101**). Otherwise, the first node **11** will abort the authentication process as described above (Block **100**) and thus will not

authenticate or send any message data to the second node **12**. Further method aspects of the invention will be apparent to those of skill in the art based upon the above description and will therefore not be discussed further herein.

5 Many modifications and other embodiments of the invention will come to the mind of one skilled in the art having the benefit of the teachings presented in the foregoing descriptions and the associated drawings. Therefore, it is understood that the invention is not to be
10 limited to the specific embodiments disclosed, and that modifications and embodiments are intended to be included within the scope of the appended claims.

CLAIMS

1. A mobile ad-hoc network comprising:
a first node for generating an authentication
5 request, said first node having a first public key and a
first private key associated therewith; and
a second node having a second public key and a
second private key associated therewith;
said first node receiving a certificate of
10 authenticity responsive to the authentication request, the
certificate of authenticity being generated by a certifying
authority and comprising the second public key, the
certifying authority having a public authentication key and a
private authentication key associated therewith and
15 generating the certificate of authenticity using the private
authentication key;
said first node decrypting the certificate of
authenticity using the public authentication key and
verifying that the second public key belongs to said second
20 node based upon the decrypted certificate of authenticity;
said first node sending challenge data to said
second node upon verification that the second public key
belongs to said second node;
said second node encrypting the challenge data
25 using the second private key and returning the encrypted
challenge data back to said first node;
said first node decrypting the encrypted challenge
data using the verified second public key and authenticating
said second node if the decryption of the encrypted challenge
30 data yields the original challenge data.

2. The mobile ad-hoc network of Claim 1 wherein
the certificate of authenticity further comprises a node
identification (ID) of the second node.

3. The mobile ad-hoc network of Claim 2 wherein said first node verifies the second public key belongs to said second node by:

5 processing the second node ID and the second public key to create a digest; and
comparing the digest with the decrypted certificate of authenticity to verify that the second public key belongs to said second node.

10 4. The mobile ad-hoc network of Claim 1 wherein said first node sends a session key encrypted with the second public key to said second node for use with subsequent data transfers therebetween upon authenticating said second node.

15 5. A mobile ad-hoc network node having a first public key and a first private key associated therewith and comprising:

a wireless communications device; and
a controller cooperating with said wireless
20 communication device for establishing a wireless communications link to an unauthenticated node having a second public key and a second private key associated therewith, said controller also for
generating and sending an authentication
25 request to the unauthenticated node via the wireless communications link,
receiving a certificate of authenticity from the unauthenticated node via the wireless communications link, the certificate of
30 authenticity being generated by a certifying authority and comprising the second public key, the certifying authority having a public authentication key and a private authentication key associated therewith and generating the

certificate of authenticity using the private authentication key,

decrypting the certificate of authenticity using the public authentication key and verifying that the second public key belongs to the unauthenticated node based upon the decrypted certificate of authenticity,

sending challenge data to the unauthenticated node via the wireless communications link upon verification that the second public key belongs to the unauthenticated node,

receiving encrypted challenge data from the unauthenticated node via the wireless communications link and decrypting the encrypted challenge data using the verified second public key, and

authenticating the unauthenticated node if the decryption of the encrypted challenge data yields the original challenge data.

6. The mobile ad-hoc network node of Claim 5 wherein said controller sends a session key encrypted with the second public key to the unauthenticated node via the wireless communications link for use with subsequent data transfers therebetween upon authenticating the unauthenticated node.

7. A node authentication method for a mobile ad-hoc network comprising a plurality of nodes, the method comprising:

generating an authentication request at a first node having a first public key and a first private key associated therewith to authenticate a second node having a

second public key and a second private key associated therewith;

receiving a certificate of authenticity responsive to the authentication request at the first node, the
5 certificate of authenticity being generated by a certifying authority and comprising the second public key, the certifying authority having a public authentication key and a private authentication key associated therewith and generating the certificate of authenticity using the private
10 authentication key;

decrypting the certificate of authenticity at the first node using the public authentication key and verifying that the second public key belongs to the second node based upon the decrypted certificate of authenticity;

15 sending challenge data from the first node to the second node upon verification that the second public key belongs to the second node;

encrypting the challenge data at the second node using the second private key and returning the encrypted
20 challenge data back to the first node; and

decrypting the encrypted challenge data at the first node using the verified second public key and authenticating the second node if the decryption of the encrypted challenge data yields the original challenge data.

25

8. The method of Claim 7 further comprising sending a session key encrypted with the second public key from the first node to the second node for use with subsequent data transfers therebetween upon authenticating
30 the second node.

9. The method of Claim 8 further comprising terminating the authentication of the second node after a predetermined period.

10. The method of Claim 7 further comprising
sending the authentication request to the second node; and
wherein receiving the certificate of authenticity comprises
receiving the certificate of authenticity from the second
5 node.

1/5

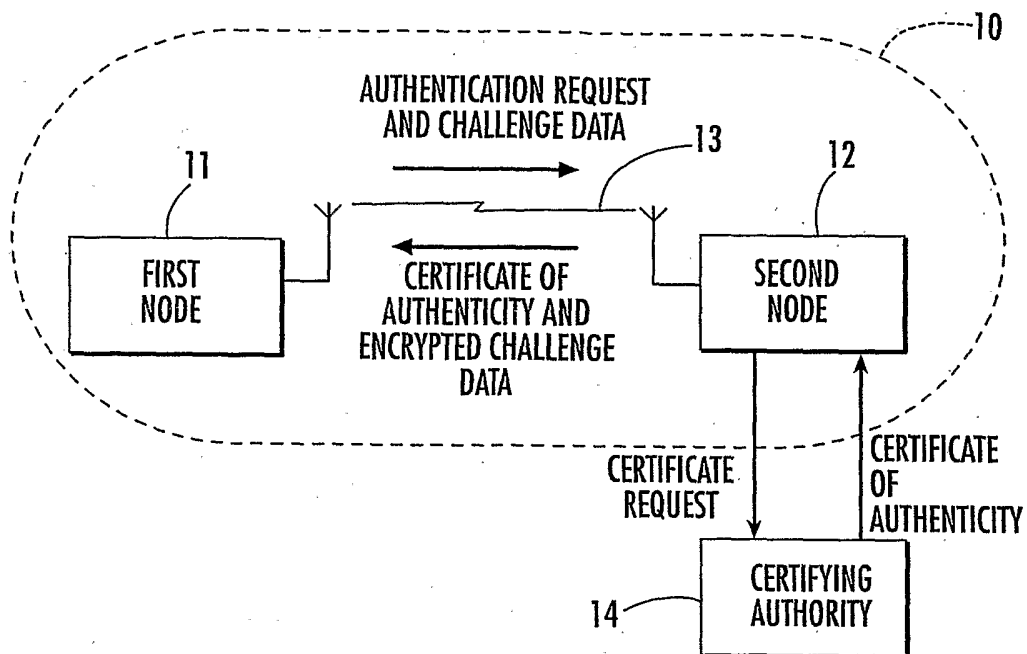


FIG. 1.

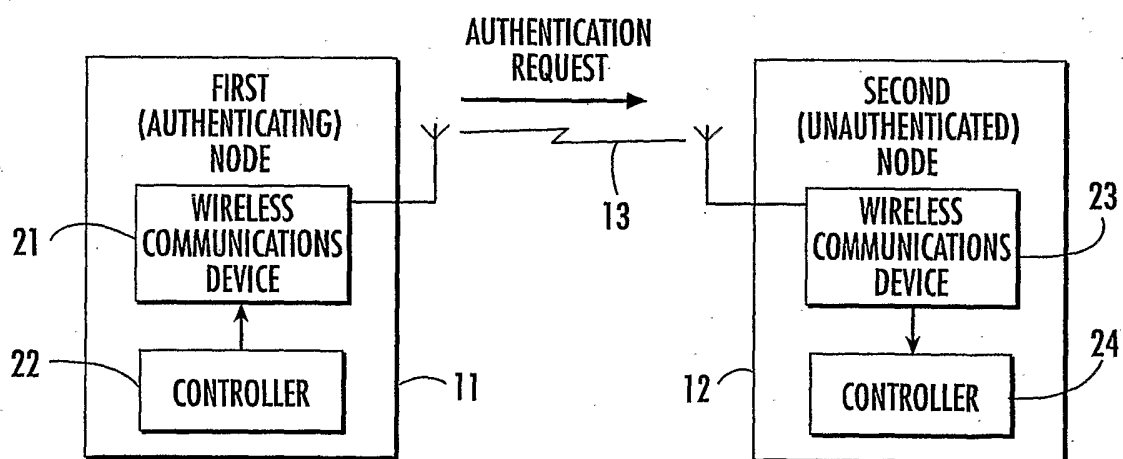


FIG. 2.

2/5

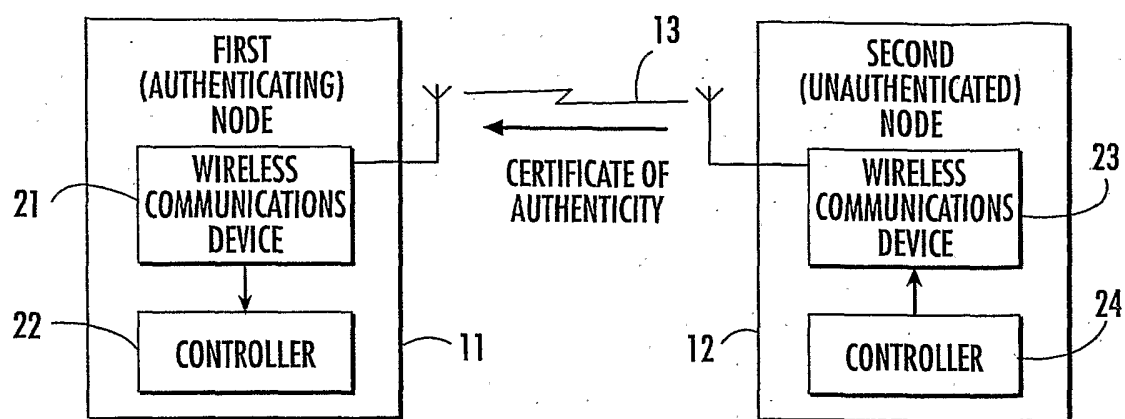


FIG. 3.

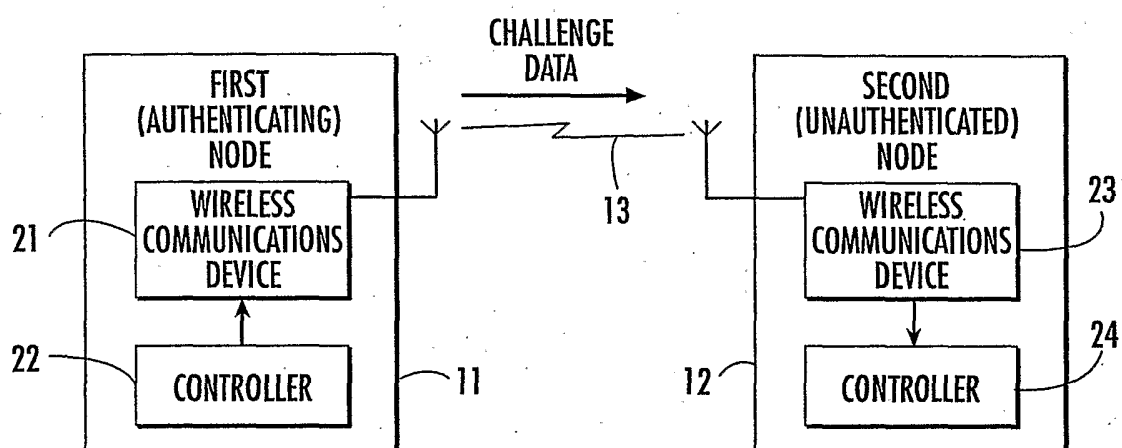


FIG. 4.

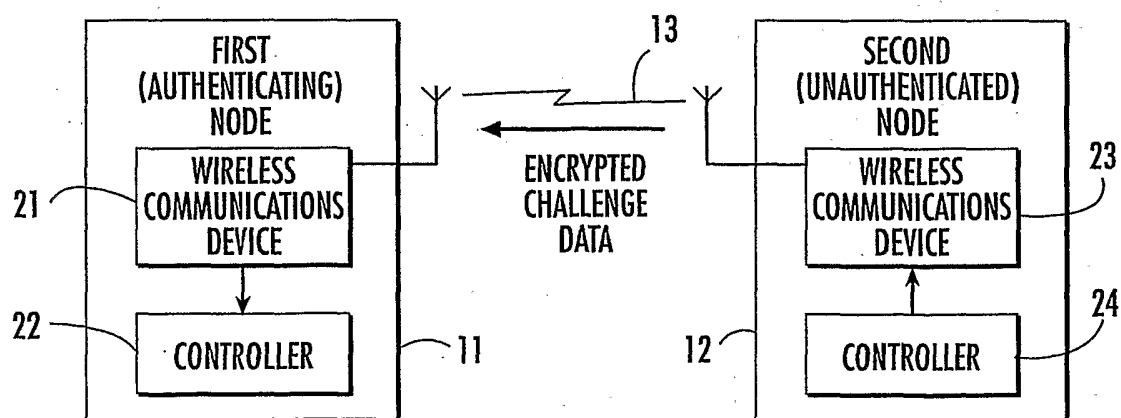


FIG. 5.

3/5

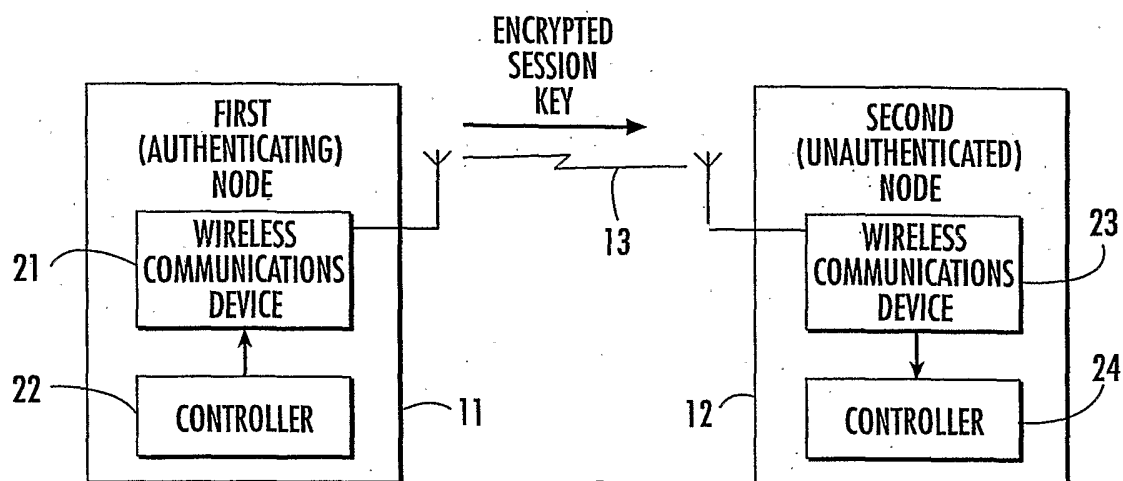


FIG. 6

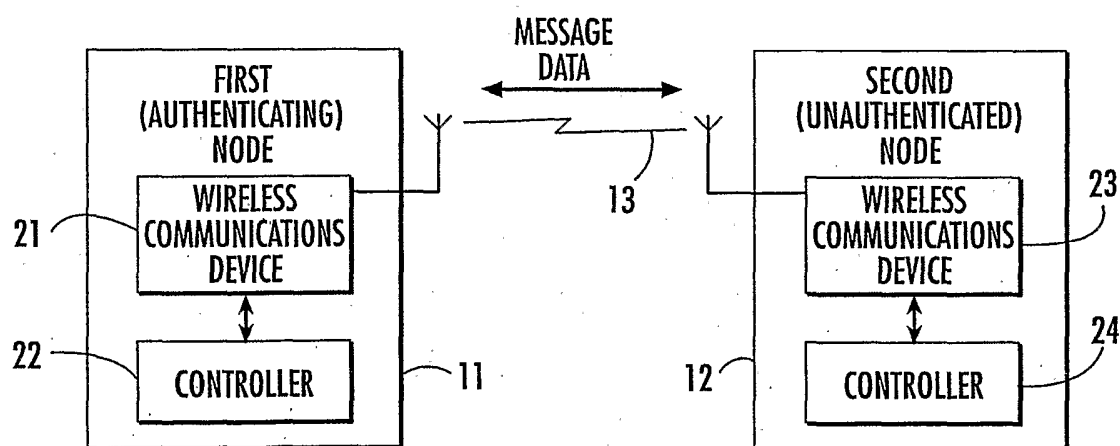


FIG. 7

4/5

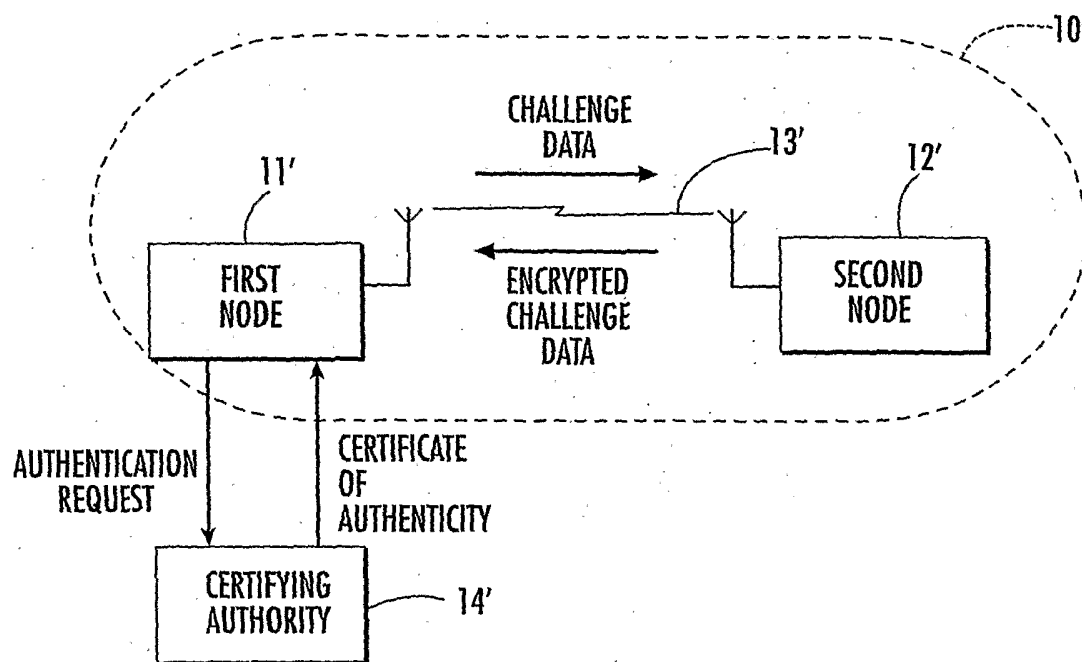


FIG. 8.

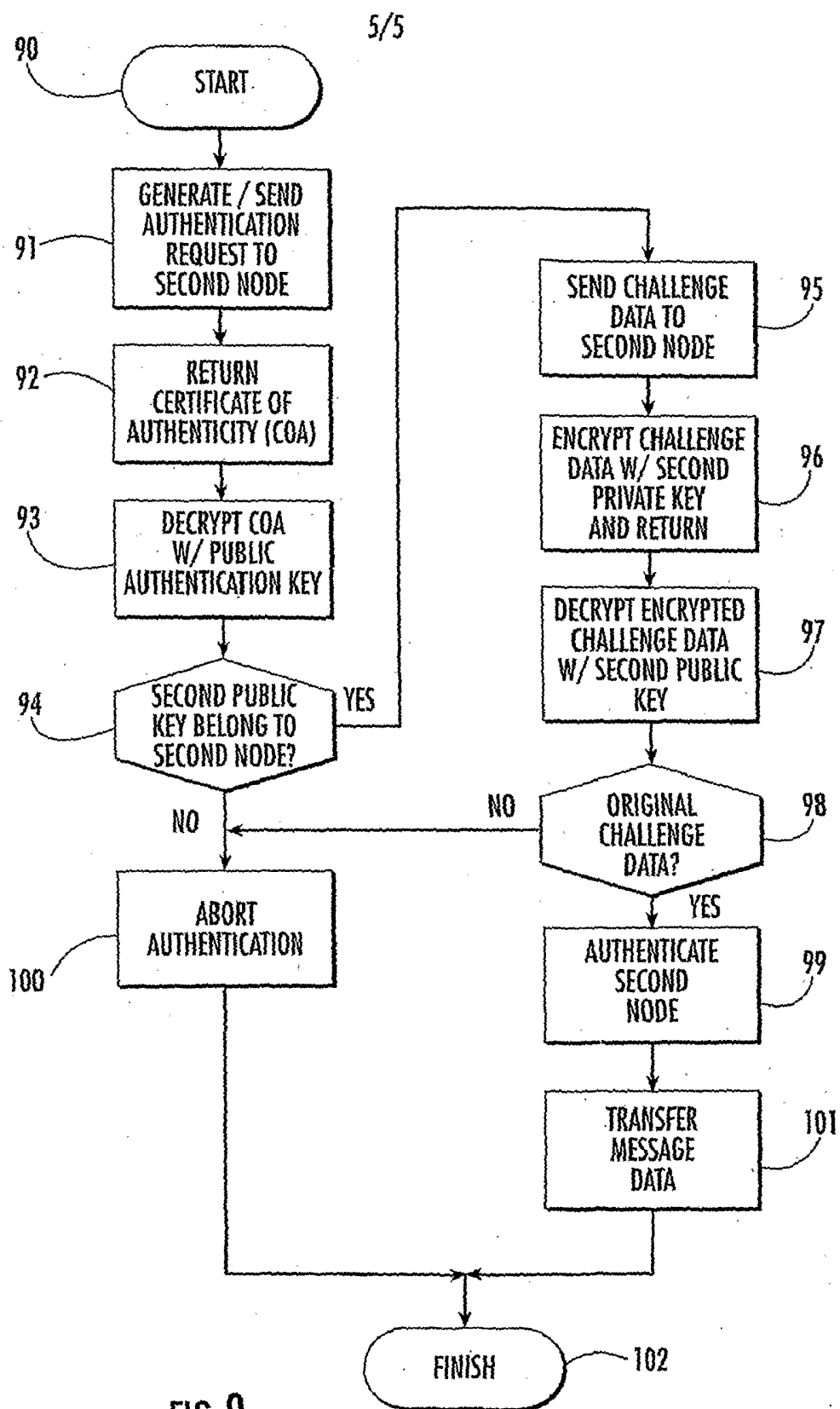


FIG. 9.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US03/20470

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) : H04L 9/00

US CL : 713/155,156,168,171

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)

U.S. : 713/155,156,168,171

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Stallings, Cryptography and Network Security 2nd Edition; Schneier, Applied Cryptography 2nd Edition.Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
East Online, Plus, ACM Online, IEEE Online**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	SCHNEIER, BRUCE; Applied Cryptography, 2nd Edition; John Wiley & Sons, Inc.; 1996; pages 47-75, 169-187.	1-10
Y	STALLINGS, WILLIAM; Cryptography and Network Security; Prentice-Hall, Inc.; 2nd Edition; 1999; pages 131-159, 173-182, 323-353, 299-319.	1-10
A	NGUYEN et al.; Security Routing Analysis for Mobile Ad Hoc Networks; Department of Interdisciplinary Telecommunications, University of Colorado at Boulder; Spring 2000.	1, 5, 7
A	ZHOU et al.; Securing Ad Hoc Networks; IEEE Network Magazine, vol. 13, no. 6; November/December 1999.	1, 5, 7
Y,P	US 6,546,425 B1 (HANSON et al) 8 April 2003 (08.04.2003), col. 6 lines 5-7.	9
A	US 5,371,794 (DIFFIE et al) 06 December 1994 (06.12.1994)	1, 5, 7
Y	US 5,402,490 (MIHM, JR.) 28 March 1995 (28.03.1995), column 2, lines 15-61. Figures 4, 6, 8, 9.	1, 2, 5, 7
A	US 5,515,441 (FAUCHER) 07 May 1996 (07.05.1996).	1, 5, 7
A	US 5,539,824 (BJORKLUND et al) 23 July 1996 (23.07.1996)	1, 4, 5, 7



Further documents are listed in the continuation of Box C.



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	"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
"E" earlier application or patent published on or after the international filing date	"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
"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)	"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
"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	"&" document member of the same patent family

Date of the actual completion of the international search

22 September 2003 (22.09.2003)

Date of mailing of the international search report

15 OCT 2003

Name and mailing address of the ISA/US

Mail Stop PCT, Attn: ISA/US
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

Facsimile No. (703)305-3230

Authorized officer

Gilberto Barron
Telephone No. (703) 305-3900

Peggy Harrod

INTERNATIONAL SEARCH REPORT

PCT/US03/20470

C. (Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5,923,756 (SHAMBROOM) 13 July 1999 (13.07.1999)	1, 5, 7
A	US 5,974,550 (MALISZEWSKI) 26 October 1999 (26.10.1999)	1, 5, 7
Y	US 6,292,896 B1 (GUSKI et al) 18 September 2001 (18.09.2001) Figure 4, 6, 11, 12, col 2, lines 44-67.	4, 8
A	US 6,405,313 B1 (REITER et al) 11 June 2002 (11.06.2002).	1, 5, 7
Y	US 6,430,690 B1 (VANSTONE et al) 06 August 2002 (06.08.2002), col. 1, line 59-col. 2, line 23.	1, 5, 7