(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) **EP 1 929 680 B1**

(12) **EUROPEAN PATENT SPECIFICATION**

(45) Date of publication and mention of the grant of the patent:
26.10.2016 Bulletin 2016/43

(21) Application number: **06802756.4**

(22) Date of filing: **29.08.2006**

(51) Int Cl.:
H04L 29/06 *(2006.01)* ***H04L 12/14*** *(2006.01)*
H04M 15/00 *(2006.01)*

(86) International application number:
PCT/US2006/034134

(87) International publication number:
WO 2007/027964 (08.03.2007 Gazette 2007/10)

(54) **METHOD AND SYSTEM FOR VERIFYING NETWORK RESOURCE USAGE RECORDS**

VERFAHREN UND SYSTEM ZUM VERIFIZIEREN VON NETZBETRIEBSMITTEL-BENUTZUNGSAUFZEICHNUNGEN

MÉTHODE ET SYSTÈME POUR VÉRIFIER DES ENREGISTREMENTS D'UTILISATION DE RESSOURCES DE RÉSEAU

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IS IT LI LT LU LV MC NL PL PT RO SE SI SK TR

(30) Priority: **02.09.2005 US 219030**

(43) Date of publication of application:
11.06.2008 Bulletin 2008/24

(73) Proprietor: **Jones, Adrian**
New York, 10069 (US)

(72) Inventor: **Jones, Adrian**
New York, 10069 (US)

(74) Representative: **Carpmael, Robert Maurice Charles et al**
Marks & Clerk LLP
90 Long Acre
London WC2E 9RA (GB)

(56) References cited:
EP-A2- 1 014 646
WO-A1-2004/062193
JP-A- 10 190 737
US-A1- 2002 188 562
US-A1- 2005 177 515

EP 1 929 680 B1

Printed by Jouve, 75001 PARIS (FR)

Description

Definitions

[0001] Network Resource: any service or facility that can be made available and accepted for use or delivery by digital transmission over a network, even if actual fulfilment is carried out by some alternate means. May include Internet or other network access, data storage and data processing, among others.

[0002] Network Resource Access Gateway ("Access Gateway"): the device (or collection of devices) that controls access to Network Resources of any kind (e.g. access point, wireless gateway, router, wireless router, switch, application gateway, etc.)

[0003] Network user device ("Device"): any network-capable device (e.g. laptop computer, PDA, smartphone, video games machine, music/video player, measurement instrument, digital camera, etc.) that can connect to a network via a Network Resource Access Gateway and make use of any Network Resource.

[0004] Network Resource User ("User"): Any person or entity that uses or controls a Network user device to gain access to Network Resources via a Network Resource Access Gateway.

[0005] Network Resource Access Gateway Operator ("Access Gateway Operator"): The operator of one or more Network Resource Access Gateways.

[0006] Network Resource Usage Statistics ("Usage Statistics"): any data that could be used for accounting and management purposes that details precisely the Network Resources used.

[0007] Billing Data: any data, however encoded, that could be used as the basis for invoicing or otherwise charging a User of Network Resources and may consist of Network Resource Usage Statistics or might be monetary (or other) data, calculated at least in part on the basis of Network Resource Usage Statistics.

[0008] Billing Service Provider: the entity that is responsible for invoicing or otherwise charging a Network Resource User for Network Resources used and for corresponding settlement of payments due to Network Resource Access Gateway Operators using billing data.

[0009] Network Resource AAA System ("AAA System"): the system responsible for authenticating Network Resource Users, authorizing their access to particular Network Resources and accounting for those Network Resources utilized; usually operated by the Billing Service Provider.

Background of the Invention

[0010] There are an increasing number of network environments where Network Resource access infrastructure is operated independently of the Billing Service Provider that maintains the accounting/billing relationship with the Network Resource User. This happens especially in the unregulated wireless network access spectrum (e.g. 802.11a/b/g, etc.) where a growing number of Users of wireless-capable Devices are accessing the Internet via independent 'wireless hotspot' operators who, in turn, have authorization and settlement arrangements with the Users' Billing Service Providers. Where the User has no direct commercial relationship with the wireless hotspot operator, these arrangements are often known as 'roaming agreements'. Whenever a User accesses the Internet via a wireless hotspot, the hotspot's operator (or their equipment) is usually responsible for sending Network Resource Usage Statistics to the Billing Service Provider, detailing information such as identity of the User, date/time of initial connection, type of Network Resource used, length of time connected, amount of data transferred, etc., so that the Billing Service Provider may charge the User correctly and also remunerate the hotspot operator for use of their Network Resource access infrastructure. Although most of this accounting is carried out automatically, using standard Authentication, Authorization and Accounting (AAA) protocols such as RADIUS (RFC 2865/2866) and DIAMETER (RFC 3588) and accounting protocols such as CRANE (RFC 3423), CIBER, TAP and IPDR (ipdr.org), which include provision for encrypted data transfer, it remains possible for the hotspot operator to manipulate their system (through software and/or hardware modifications) so that Network Resource Usage Statistics are exaggerated in their favour (e.g. by inflating the reported amount of data transferred, overstating the length of connection or misreporting the type of resource used, etc.). This is a serious issue because it is almost impossible for the Billing Service Provider to detect fraud of this type using present standards and technologies. The Billing Service Provider is almost entirely limited to carrying out audit-style spot-checks to try to detect any inaccurate reporting. Even assuming such spot-checks can be carried out without detection as such, they are costly to undertake and prone to miss many cases of inaccurate reporting, particularly where it is not constant. The Network Resource User is also extremely unlikely to notice any discrepancy unless the fraud is egregious and the User is able to check against any connection logs that may have been created by their Device. The potential for fraud becomes far more serious as an ever increasing number of Network user device Users access chargeable Network Resources via Access Gateway Operators who are independent of their Billing Service Providers.

Prior Art

[0011] The prior art has done little to address this problem, for good reason: In the traditional telecommunications model (whether conventional fixed line or mobile telephony, data networking or ISP), the Billing Service Provider is also usually the Access Gateway Operator. The Billing Service Provider therefore implicitly trusts the Network Resource Usage Statistics transmitted to its AAA System by the Access Gateway. In some business

models, such as is the case with some ISPs and "virtual" telecommunications operators, the Billing Service Provider enters into agreements with other telecommunications companies who operate the Access Gateways (e.g. distributed banks of dial-in modems, cellular telephony base stations or remote wireless access gateways). There is usually little concern in these situations that the Access Gateways will be manipulated to generate fraudulent Network Resource Usage Statistics, since the operators are large companies with (generally) good reputations to protect. However, the *potential* for fraud has been widely recognised, including in some of the Internet's standards documents in this area, and some measures have been taken to help protect against it. For example, in May 1999, Zorn, G. and Calhoun, P. published a paper, "Limiting Fraud in Roaming", (available as: draft-ietf-roamops-fraud-limit-00.txt) as an IETF work-in-progress, highlighting different methods of potential fraud that remain possible in today's network infrastructure (particularly in relation to the widely-used RADIUS protocol) and some possible solutions. The IETF's latest standard for Authentication, Authorization and Accounting - that for Diameter (RFC 3588), published in 2003 - attempts to address some elements of potential accounting fraud. Under section 1 (introduction) of the standard, there is a sub-section on 'Auditability'. It has the following paragraph about RADIUS:

[0012] RADIUS does not define data-object security mechanisms, and as a result, untrusted proxies may modify attributes or even packet headers without being detected. Combined with lack of support for capabilities negotiation, this makes it very difficult to determine what occurred in the event of a dispute. While implementation of data object security is not mandatory within Diameter, these capabilities are supported, and are described in [AAACMS].

[0013] In both Diameter and proprietary developments, the recent prior art has focused on maintaining the security and integrity of Network Resource Usage Statistics during transmission between the Access Gateway and the Billing Service Provider. For example, while Diameter supports optional implementation of data object security, it only does so to prevent untrusted intermediate proxy servers from modifying the accounting data. It does not address the other fundamental issue of how you ensure the accuracy of the original accounting data in the first place - and how you can audit it. If the Access Gateway generates Network Resource Usage Statistics based on a validly authenticated and authorized User, use of the prior art only ensures that these records can be transmitted back to the Billing Service Provider without meaningful risk of undetected modification.

[0014] Under the prior art, Figure 1 illustrates (in overall terms) how an Access Gateway typically accounts for a Network user device's Network Resource usage:

1) The Access Gateway receives a request from a Network user device to provide access to some kind of Network Resource (e.g. Internet access). Ordinarily, the Network user device sends some form of credentials as part of this request (e.g. user name, hashed password, service required, etc.)

2) The Access Gateway then makes a request of the AAA System to determine whether service may be provided to the User and Device.

3) The Access Gateway receives a response from the AAA System. Provided the response is positive, the process continues.

4) The Access Gateway makes the authorized Network Resource available to the Network user device. It also (ordinarily) notifies the AAA System that it is starting accounting for the Network user device's Network Resource consumption.

5) The Access Gateway deals with network traffic to/from the Network user device in accordance with the Network Resource authorized for use, while keeping track of the Network user device's Network Resource consumption by recording Network Resource Usage Statistics.

6) The Access Gateway receives a request to terminate the current communications session from the Network user device. Termination may also occur for a number of alternative reasons, including: i) the Access Gateway's timers record a sufficient period of inactivity to terminate the session as a timeout; ii) the Access Gateway detects termination of the connection by the Network user device without a formal request; iii) notification is received from the AAA System that the session must be terminated (e.g. due to the user's credit limit being reached) and IV) the Access Gateway's administrator instructs termination of the session.

7) The Access Gateway generates an Accounting Record (Network Resource Usage Statistics) containing details of the Network Resources consumed by the Network user device and sends it to the AAA System.

[0015] Traffic between the Access Gateway and AAA System may pass between any number of proxy servers. The prior art can provide what is currently considered adequate protection to prevent tapering with data transmitted between these components by using end-to-end encryption and transmissions protocols that are resistant to man-in-the middle attacks and replays,

[0016] In the evolving world of unregulated WiFi roaming, where Access Gateways can be anywhere and operated by anyone, the potential for fraud at the point of generating the Network Resource Usage Statistics has increased substantially. Many WiFi 'hotspot' operators are small businesses or individuals without necessarily the same reputations or credentials as the larger telecommunications companies. Currently, some companies that operate as Billing Service Providers in this field (e.g. iPass, Boingo, etc.), use audit-style spot-checks to

test the validity of Network Resource Usage Statistics from different Access Gateway Operators that they have direct or indirect commercial arrangements with. The spot-check test User will undertake one or more sessions accessing Network Resources from a Network user device via an Access Gateway and keep a detailed log of Network Resource usage by the Network user device. The resulting data is later compared with the data logged with the Billing Service Provider to check for accuracy.

[0017] US2004/062193 A1 discloses a method for billing a communication connection, which is established via the Internet between a first communication terminal and a mobile target communication device of a packet-oriented mobile radio network. According to said method: a connection request message relating to the communication connection is routed from the first communication terminal to a network node of the mobile radio network via the Internet, a billing computer containing stored charge payment data relating to the first communication terminal inserts a data structure relating to the charges to be borne by the billing computer into the connection request message or another message that is routed from the first communication terminal to the network node of the mobile radio network via the Internet; the network node of the mobile radio network verifies the validity of the data structure and if the result is positive, the communication connection with the target communication terminal in said network is established, or if the result is negative, the establishment of the communication connection in the mobile radio network is rejected.

[0018] JP 10 190737 A discloses a system whereby encryption of billing data is enabled, so tampering of such data can be detected.

Summary of the Present Invention

[0019] The present invention provides a system as claimed in claim 1 and a method as claimed in claim 7. Preferred embodiments are covered by the appended dependent claims.

Summary of the Problem

[0020]

1. Referring to Figure 2, each of the parties depicted operates with independent commercial motives.

2. The User ("U") is concerned that the Access Gateway Operator ("A"), who he may not know or trust, will try to overcharge him by inflating the record of his Network Resource usage sent to the Billing Service Provider ("B"). However, the User has chosen to trust B and has entered into a commercial relationship with him.

3. The Access Gateway Operator is concerned that the User, who he may not know or trust, will somehow try to dispute his accurate record of Network Resource usage sent to the Billing Service Provider. However, the Access Gateway Operator has chosen to trust B and has entered into a commercial relationship with him.

4. The Billing Service Provider does not trust either the Access Gateway Operator or the User independently but his responsibility is to settle charges between them. If both A and U agree on the type and quantity of Network Resource used (and B is confident that their agreement cannot have been tampered with), then B trusts their mutual agreement.

Brief Summary

[0021]

U does not trust A
A does not trust U
U trusts B
A trusts B
B does not trust U or A independently except if they demonstrate mutual agreement

Communications

[0022]

U can communicate directly to A
A can communicate directly to U
U can only communicate to B via A
B can only communicate to U via A

[0023] Any situation where information has to be passed via an untrusted intermediary causes potential issues of integrity. Even when using a strong cryptosystem, communications between U and B and B and U are susceptible to various forms of substitutions, replays or man-in-the-middle attacks. A is a man-in-the-middle with a potential commercial incentive to commit such an attack.

[0024] The present invention differs from US2004/062193 in that the access gateway of the present invention is not a trusted component for transmitting billing data and therefore a system and method are provided for ensuring that the billing data can be independently verified as representing the agreed utilisation of network resources between a network user device and an access gateway.

Brief Description of the Drawings

[0025]

Figure 1 illustrates how an Access Gateway accounts for a Network user device's Network Resource usage according to the prior art.

Figure 2 is a block overview diagram showing the relationship of the Access Gateway to system which provides network access and accounting for Network Resource usage.

Figure 3 illustrates how an Access Gateway accounts for a Network user device's Network Resource usage according to the present invention.

Detailed Description of the Invention

[0026] The present invention is based on the premise that if two parties to a transaction who do not trust each other agree on a detailed record of that transaction - and that record cannot later be modified without detection - then the agreed details of the transaction cannot later be repudiated by either party. More specifically, in the case of a Network Resource usage transaction, where the details of the transaction are changing over time (as Network Resources are consumed over time) and either party can unilaterally walk away from the transaction in progress (by dropping the connection without prior notification to or agreement of the other party), the only record of the transaction that is guaranteed not to be repudiated by either party, is their latest agreement on the then-outstanding state of the transaction.

[0027] The present invention therefore involves improvements to Access Gateway 11 enabling it to keep track of the latest state of agreement between it and the Network user device 13 for Network Resources consumed during a session utilizing Network Resources (such as utilization of a network 15 or storage attached to a network 15). This dynamic state of agreement is updated periodically during the network session and is non-modifiable by the Access Gateway without later being detectable. An AAA system 17 utilized by a Billing Service Provider authenticates Users and their access to Network Resources using network 15.

[0028] Figure 3 illustrates the principal changes to the prior art under the present invention:

[0029] Steps 1-5 are exactly the same as for the prior art shown in Figure 1. Step 8a is the same as Step 6 for the prior art, except for where there is an explicit termination of session by the Network user device, in which case, it is as detailed below. Step 9 is the same as Step 7 of the prior art. Also shown in Figure 3 are the necessary new steps 6a, 7a and 10:

[0030] 6a) From time-to-time during the session, typically, approximately every 10 seconds (though entirely dependent on the requirements of the specific implementation to reflect factors such as the cost and volume of Network Resources utilized), the Access Gateway receives from the Network user device Billing Data that is a function of the Network user device's record of Network Resource Usage Statistics for one or more parameters of its Network Resource consumption through the Access Gateway, referenced off some commonly known base point (preferably, start of current session). The Access Gateway has some means, such as by decoding the received billing data using the Network user device's public key, of reading one or more parameters in the received billing data, so that it can determine whether one or more of the parameters correlate(s) with the Access Gateway's own record of those parameters. In determining the correlation (e.g. comparison of time connected or volume of data transferred), the Access Gateway may take into account the latency involved in generating and transmitting the billing data. More specifically, it would need to determine whether the received parameter(s) is/are within the specific range of values that would be expected by the Access Gateway when allowing for the time delays (typically, from a few milliseconds up to 1-2 seconds) that would have occurred due to data processing by the network user device (including encoding) and network latency. In some cases (e.g. if connection time was the Network Resource being reported every 10 seconds), the expected range of values would only be a single value (i.e. in the previously mentioned case, the Access Gateway's current session time counter, rounded down to the nearest 10 seconds). The received billing data, while containing one or more parameters that are readable by the Access Gateway, must contain at least one portion encoded in such a fashion that those parameter(s) may not be modified or replaced (including by all or part of a previous session's billing data) without later detection being possible by a qualified third-party (e.g. one that holds, among other things, a corresponding secret to the one used by the Network user device to encode the data). While the prior art for suitable encoding methods is well understood, several possible encoding methods are detailed below. In the prior art, when spot-check audits are carried out using remote devices keeping connection logs, a similar comparison is undertaken (without requiring any special form of encoding), though not until after the network resource usage session has terminated, as that is the first time when the access gateway's network resource usage statistics become available in the prior art (in the form of an accounting record). This invention depends on the comparison occurring actively during network resource usage, since the amount of network resource used might otherwise later be repudiated. If the access gateway disagrees with what it receives (from a Network User Device) during an active session, then it has the ability to terminate the active network resource usage immediately.

1) If the Access Gateway determines that the parameters (or any derivatives thereof) included in newly received billing data do not correlate with its own record or calculation of those parameters (e.g. it appears that the Network user device is understating its consumption of Network Resources), then the Access Gateway may terminate the session. If the Access Gateway concurs with the received parameter(s), then it stores the received billing data (or at least one or more of its encoded parameters) and

continues to provide service to the Network user device.

2) If the Access Gateway does not receive billing data relating to a parameter that it is expecting within an anticipated timeframe, then the Access Gateway may terminate the session. (For example, the Access Gateway, may be required to obtain up-to-date billing data after every 10 seconds of connection time. If it has not received such data after 12 seconds, which allows a grace period for the Network user device to generate the data and for subsequent latency in network transmission, the Access Gateway may terminate the session).

3) It should be noted that the received Billing Data may consist of or contain, in a suitably encoded format, one or more of the following:

Some or all of the network resource usage statistics; or

A derivation from some or all of the network resource usage statistics; or

A (digitally signed) "payment" or "authorization" acknowledgement that relates to the consumption of network resource (i.e. agreed to purchase X units). For example, in one embodiment, the access gateway might have sent a notice to the Network User Device that it has used 30 minutes of connection time and therefore needs to acknowledge that payment for $1 is due. In this case, the Network User Device would use its own record of network resource usage statistics to confirm that 30 minutes had been used and therefore send an authorization for $1 to the access gateway, though it need not reference the network resource usage statistics. The authorization would be a function of the network resource usage but would not necessarily be directly derived from it.

[0031] 7a) Step 7a is a repetition of step 6a. The Access Gateway continues to receive Billing Data from the Network user device during the session and processes it as in step 6a. The frequency with which the Billing Data is received by the Access Gateway depends on implementation and configuration. In one embodiment, at authorization of the session, the Access Gateway would receive notification from the AAA System of which parameters were to be tracked as Network Resource Usage Statistics and with what frequency. It would also pass these parameters on to the Network user device. In other embodiments, the parameters and frequency may be preset or pre-configured into the Access Gateway and Network user device.

[0032] If the Access Gateway receives a formal session termination notification from the Network user device, it may also receive one or more corresponding sets of Billing Data earlier than otherwise anticipated. It processes these in the same manner as step 6a.

[0033] The Access Gateway forwards to the AAA System (directly or indirectly) the most recently received and verified (i.e. correlated) billing data - or at least predetermined portions thereof - in the encoded form as received from the Network user device.

[0034] More specifically, the forwarded data must include at least sufficient portions of encoded billing data (forwarded in a format compatible with the receiving AAA System) such that the AAA System can verify that this data could only have originated from the User's network user device (and that any specific parameters encoded therein have not been modified) and such that the AAA System would have sufficient data to compare any billing data that needs to be verified with corresponding accounting data or other billing data generated by the Access Gateway and also forwarded to the AAA System. If more than one Network Resource is being monitored, then multiple sets of billing data (or portions thereof) may be forwarded by the Access Gateway to the AAA System.

Encoding Methods

[0035] To ensure that the Billing Data received by the Access Gateway from the Network user device may not be tampered with by the Access Gateway without later being detectable by the AAA System, a special method of encoding at least one portion of the billing data must be employed. The Billing Data must consist of or contain the result(s) of one or more transformation functions that are dependent on both the parameters that need to be non-modifiable and a secret key that is unknown to (and computationally infeasible to determine) the Access Gateway. The transformation function can be any function where it is computationally infeasible to determine the result of the transformation function for one or more chosen parameter values without knowledge of the secret key. The encoded portion(s) of Billing Data must also incorporate provision to prevent previously valid (encoded) Billing Data from being reused (i.e. in what would commonly be referred to in cryptography as a replay attack). Such provision could be provided, for example, by incorporating one or more of a unique session identifier and/or timestamp into the portion(s) of Billing Data prior to encoding. Safe methods of generating and managing such anti-replay 'keys' and ensuring that later detection or reused data is possible are well understood and beyond the scope of this invention.

[0036] The following examples illustrate alternate encoding methods and their relative advantages and disadvantages for different implementation scenarios:

Asymmetric (public key) Cryptography Data Encoding

[0037] The data is encoded by the Network user device using the User's private (secret) key.

[0038] It can be decoded by the Access Gateway using the User's public key, which would need to be provided to the Access Gateway as part of the implementation protocol.

[0039] Advantages: Compactness of data that is received/transmitted over the network; no risk of secret key leakage from the Billing Service Provider.

[0040] Disadvantages: Requirement to deliver the User's public key to the Access Gateway at initiation of the session; relatively high processing requirement to support currently-known forms of asymmetric cryptography.

Plaintext with Digitally Signed Hash

[0041] The data is encoded by the Network user device appending to the plaintext (unencrypted) data a digitally signed hash created using the plaintext data and the User's private (secret) key.

[0042] The Access Gateway can read the plaintext data without any additional requirements, though cannot modify it without causing the digitally signed hash to become invalidated. The Access Gateway can check the validity of the digitally signed hash by generating its own hash of the plaintext and comparing it with the digitally signed hash decoded by using the User's public key (which would need to be provided to the Access Gateway as part of the implementation protocol).

[0043] Advantages: Potentially higher performance than encryption of all the plaintext data.

[0044] Disadvantages: Increased length of the encoded data, creating slightly higher level of network traffic.

Symmetric Cryptography

[0045] While symmetric cryptography using a secret key unknown to the Access Gateway could be used in this invention as an encoding method for portions of the received billing data (e.g. to encrypt a hash of plaintext along with plaintext data), it is not a preferred method of encoding. The main reason for this is that it would make it impossible for the Access Gateway to determine with certainty that the received billing data correlated fully with its own billing data, even if the portions that it could read did so (e.g. the plaintext might correlate but the encrypted hash might not). Providing all the Billing Data (both received and that generated by the Access Gateway) were forwarded to the AAA System, patterns of fraudulent activity might be picked up and it would likely be possible to determine over multiple sessions across different Access Gateways whether it were a rogue Access Gateway modifying received Billing Data or a rogue Network User Device submitting inconsistent Billing Data, but this would not be possible for any single Network Resource usage session, so the value of the invention would be diminished.

[0046] Of course, prior to a User being able to initiate a session using Network Resources, the Access Gateway would have contacted the AAA System to authenticate a connection from the Network User Device's User. If the AAA System determined that the Access Gateway was untrusted (e.g. operated by a third-party), a protocol for establishing an authenticated connection would need to be implemented. However, the details of such a protocol are not needed for a proper understanding of the invention as defined by the following claims.

Claims

1. A system for avoiding potentially fraudulent network resource usage, the system comprising:

   means for generating billing data based at least in part on network resource usage statistics;
   means for receiving said generated billing data in tamper-evident encoded form:
   means for decoding said received billing data and comparing said decoded billing data with corresponding billing data generated by an access gateway (11) during network resource usage; and
   means for storing predetermined portions of said received billing data if said decoded billing data correlates to said corresponding billing data; and
   means for terminating said network resource usage if said decoded billing data does not correlate to said corresponding billing data.

2. The system defined by Claim 1 wherein said access gateway transmits said predetermined portions of said received billing data to said billing service provider.

3. The system defined by Claim 2 where said received billing data is the most recently received billing data.

4. The system defined by Claim 1 wherein said means for decoding performs one of asymmetric cryptography data decoding, and digitally signed hash decoding from plaintext with digitally signed hash.

5. The system defined by Claim 1 further comprising means for transmitting notification of non-correlation of said received billing data with said corresponding billing data to a billing service provider.

6. The system defined by Claim 5 wherein said transmitted notification includes predetermined portions of at least one of said received billing data and said corresponding billing data.

7. A method for generating independently verifiable billing data said method comprising:

   generating billing data based at least in part on

network resource usage statistics;
receiving said generated billing data in tamper-evident encoded form; decoding said received billing data and comparing said decoded billing data with corresponding billing data generated by an access gateway (11) during network resource usage;
if said decoded billing data correlates to said corresponding billing data, storing predetermined portions of said received billing data; and
if said decoded billing data does not correlate to said corresponding billing data, terminating said network resource usage

8. The method defined by Claim 7 where said decoding is one of asymmetric cryptography data decoding and digitally signed hash decoding from plaintext with digitally signed hash.

9. The method defined by Claim 7 further comprising transmitting said predetermined portions of said received billing data to a billing service provider.

10. The method defined by Claim 7 where said received billing data is the most recently received billing data.

11. The method defined by Claim 9 further comprising transmitting notification of non-correlation of said received billing data with said corresponding billing data to a billing service provider.

12. The method defined by Claim 11 wherein said notification includes predetermined portions of at least one of said received billing data and said corresponding billing data

Patentansprüche

1. System zum Vermeiden einer möglicherweise betrügerischen Verwendung von Netzwerkbetriebsmitteln, das System umfassend:

ein Mittel zum Erzeugen von Rechnungsstellungsdaten basierend mindestens teilweise auf Netzwerkbetriebsmittel-Verwendungsstatistiken;
ein Mittel zum Empfangen der erzeugten Rechnungsstellungsdaten in manipulationsgeschützter codierter Form;
ein Mittel zum Decodieren der empfangenen Rechnungsstellungsdaten und Vergleichen der decodierten Rechnungsstellungsdaten mit korrespondierenden, von einem Zugangsgateway (11) während der Verwendung der Netzwerkbetriebsmittel erzeugten Rechnungsstellungsdaten; und
ein Mittel zum Speichern im Voraus bestimmter Abschnitte der empfangenen Rechnungsstellungsdaten, wenn die decodierten Rechnungsstellungsdaten mit den korrespondierenden Rechnungsstellungsdaten korrelieren; und
ein Mittel zum Beenden der Verwendung der Netzwerkbetriebsmittel, wenn die decodierten Rechnungsstellungsdaten nicht mit den korrespondierenden Rechnungsstellungsdaten korrelieren.

2. System nach Anspruch 1, wobei der Zugangsgateway die im Voraus bestimmten Abschnitte der empfangenen Rechnungsstellungsdaten an den Rechnungsstellung-Dienstanbieter überträgt.

3. System nach Anspruch 2, wobei die empfangenen Rechnungsstellungsdaten die zuletzt empfangenen Rechnungsstellungsdaten sind.

4. System nach Anspruch 1, wobei das Mittel zum Decodieren eines von asymmetrischer Kryptographie-Datendecodierung und digital signierter Hash-Decodierung aus Klartext mit digital signiertem Hashwert durchführt.

5. System nach Anspruch 1, ferner umfassend ein Mittel zum Übertragen einer Benachrichtigung über Nichtkorrelation der empfangenen Rechnungsstellungsdaten mit den korrespondierenden Rechnungsstellungsdaten an einen Rechnungsstellung-Dienstanbieter.

6. System nach Anspruch 5, wobei die übertragene Benachrichtigung im Voraus bestimmte Abschnitte mindestens eines der empfangen Rechnungsstellungsdaten und der korrespondierenden Rechnungsstellungsdaten enthält.

7. Verfahren zum Erzeugen von unabhängig verifizierbaren Rechnungsstellungsdaten, das Verfahren umfassend:

Erzeugen von Rechnungsstellungsdaten basierend mindestens teilweise auf Netzwerkbetriebsmittel-Verwendungsstatistiken;
Empfangen der erzeugten Rechnungsstellungsdaten in manipulationsgeschützter codierter Form;
Decodieren der empfangenen Rechnungsstellungsdaten und Vergleichen der decodierten Rechnungsstellungsdaten mit korrespondierenden, von einem Zugangsgateway (11) während der Verwendung der Netzwerkbetriebsmittel erzeugten Rechnungsstellungsdaten;
wenn die decodierten Rechnungsstellungsdaten mit den korrespondierenden Rechnungsstellungsdaten korrelieren, Speichern von im Voraus bestimmten Abschnitten der empfange-

nen Rechnungsstellungsdaten; und
wenn die decodierten Rechnungsstellungsdaten nicht mit den korrespondierenden Rechnungsstellungsdaten korrelieren, Beenden der Verwendung der Netzwerkbetriebsmittel.

8. Verfahren nach Anspruch 7, wobei das Decodieren eines von asymmetrischer Kryptographie-Datendecodierung und digital signierter Hash-Decodierung aus Klartext mit digital signiertem Hashwert ist.

9. Verfahren nach Anspruch 7, ferner umfassend Übertragen der im Voraus bestimmten Abschnitte der empfangenen Rechnungsstellungsdaten an einen Rechnungsstellung-Dienstanbieter.

10. Verfahren nach Anspruch 7, wobei die empfangenen Rechnungsstellungsdaten die zuletzt empfangenen Rechnungsstellungsdaten sind.

11. Verfahren nach Anspruch 9, ferner umfassend Übertragen einer Benachrichtigung über Nichtkorrelation der empfangenen Rechnungsstellungsdaten mit den korrespondierenden Rechnungsstellungsdaten an einen Rechnungsstellung-Dienstanbieter.

12. Verfahren nach Anspruch 11, wobei die Benachrichtigung im Voraus bestimmte Abschnitte mindestens eines der empfangen Rechnungsstellungsdaten und der korrespondierenden Rechnungsstellungsdaten enthält.

Revendications

1. Système permettant d'éviter une utilisation de ressources de réseau potentiellement frauduleuse, le système comprenant :

un moyen pour générer des données de facturation sur la base, au moins en partie, de statistiques d'utilisation de ressources de réseau ;
un moyen pour recevoir lesdites données de facturation générées sous une forme codée inviolable ;
un moyen pour décoder lesdites données de facturation reçues et pour comparer lesdites données de facturation décodées à des données de facturation correspondantes générées par une passerelle d'accès (11) au cours d'une utilisation de ressources de réseau ; et
un moyen pour stocker des parties prédéterminées desdites données de facturation reçues si lesdites données de facturation décodées sont corrélées auxdites données de facturation correspondantes ; et
un moyen pour mettre fin à ladite utilisation de ressources de réseau si lesdites données de facturation décodées ne sont pas corrélées auxdites données de facturation correspondantes.

2. Système selon la revendication 1, dans lequel ladite passerelle d'accès transmet lesdites parties prédéterminées desdites données de facturation reçues audit fournisseur de services de facturation.

3. Système selon la revendication 2, dans lequel lesdites données de facturation reçues correspondent aux données de facturation reçues le plus récemment.

4. Système selon la revendication 1, dans lequel ledit moyen de décodage met en oeuvre l'un parmi un décodage de données de chiffrement asymétrique, et un décodage de hachage signé numériquement à partir de texte en clair avec un hachage signé numériquement.

5. Système selon la revendication 1, comprenant en outre un moyen pour transmettre une notification d'absence de corrélation entre lesdites données de facturation reçues et lesdites données de facturation correspondantes, à un fournisseur de services de facturation.

6. Système selon la revendication 5, dans lequel ladite notification transmise inclut des parties prédéterminées d'au moins l'une parmi lesdites données de facturation reçues et lesdites données de facturation correspondantes.

7. Procédé de génération de données de facturation vérifiables de manière indépendante, ledit procédé comprenant les étapes ci-dessous consistant à :

générer des données de facturation sur la base, au moins en partie, de statistiques d'utilisation de ressources de réseau ;
recevoir lesdites données de facturation générées sous une forme codée inviolable ;
décoder lesdites données de facturation reçues et comparer lesdites données de facturation décodées à des données de facturation correspondantes générées par une passerelle d'accès (11) au cours d'une utilisation de ressources de réseau ;
si lesdites données de facturation décodées sont corrélées auxdites données de facturation correspondantes, stocker des parties prédéterminées desdites données de facturation reçues ; et
si lesdites données de facturation décodées ne sont pas corrélées auxdites données de facturation correspondantes, mettre fin à ladite utilisation de ressources de réseau.

8. Procédé selon la revendication 7, dans lequel ledit décodage est l'un parmi un décodage de données de chiffrement asymétrique, et un décodage de hachage signé numériquement à partir de texte en clair avec un hachage signé numériquement.

9. Procédé selon la revendication 7, comprenant en outre l'étape consistant à transmettre lesdites parties prédéterminées desdites données de facturation reçues à un fournisseur de services de facturation.

10. Procédé selon la revendication 7, où lesdites données de facturation reçues correspondent aux données de facturation reçues le plus récemment.

11. Procédé selon la revendication 9, comprenant en outre l'étape consistant à transmettre une notification d'absence de corrélation entre lesdites données de facturation reçues et lesdites données de facturation correspondantes, à un fournisseur de services de facturation.

12. Procédé selon la revendication 11, dans lequel ladite notification inclut des parties prédéterminées d'au moins l'une parmi lesdites données de facturation reçues et lesdites données de facturation correspondantes.

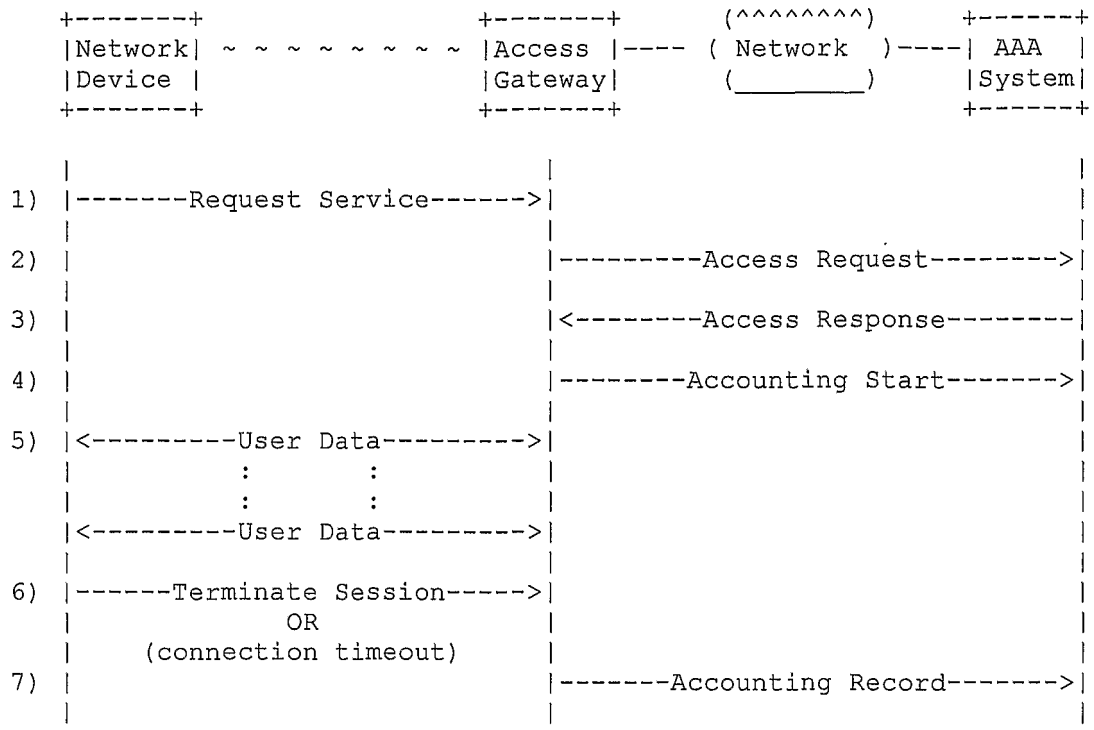

Figure 1
Prior Art

Overview Diagram

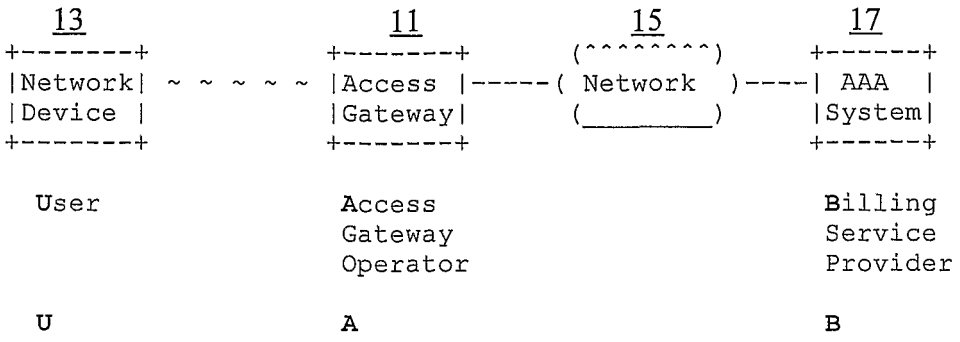

Figure 2

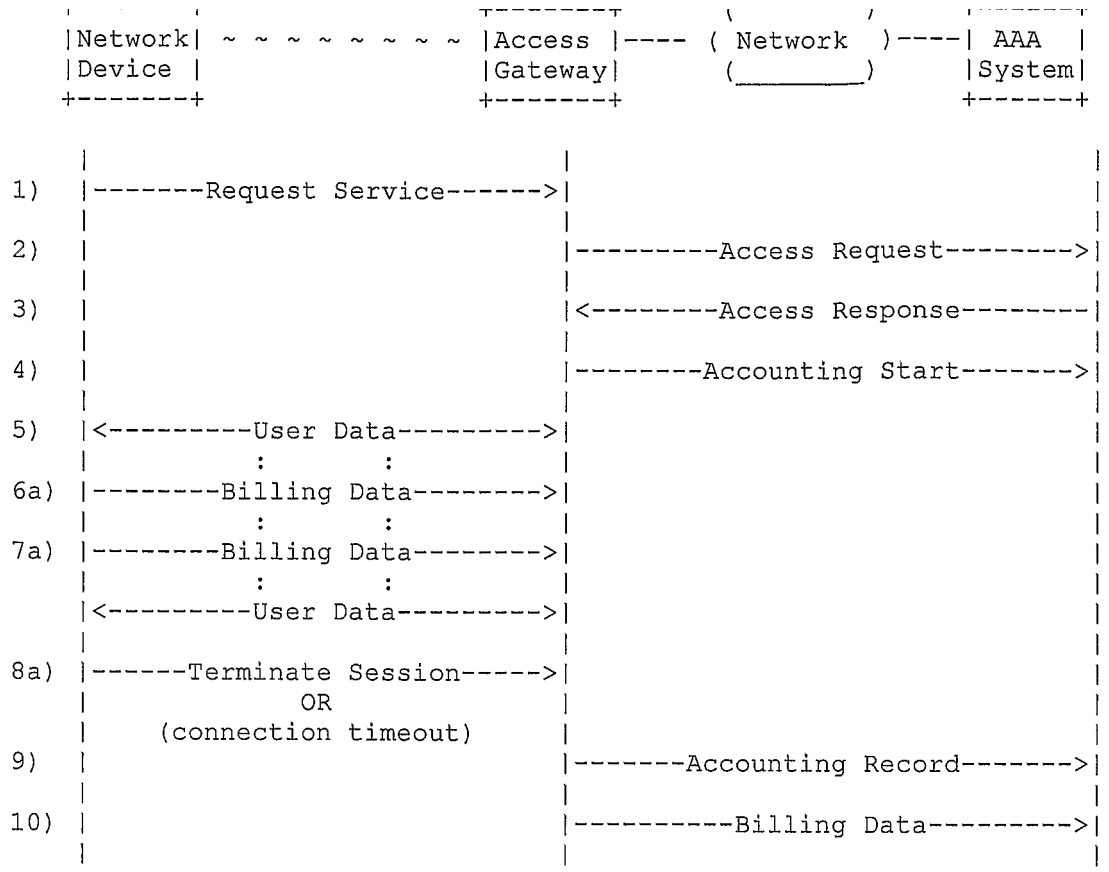
Network Device
Access Gateway
Network
AAA System
1) Request Service
2) Access Request
3) Access Response
4) Accounting Start
5) User Data
6a) Billing Data
7a) Billing Data
User Data
8a) Terminate Session
OR
(connection timeout)
9) Accounting Record
10) Billing Data

Figure 3

REFERENCES CITED IN THE DESCRIPTION

This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Patent documents cited in the description

- US 2004062193 A1 **[0017]**
- US 2004062193 A **[0024]**

Non-patent literature cited in the description

- **ZORN, G. ; CALHOUN, P.** *Limiting Fraud in Roaming,* May 1999, draft-ietf-roamops-fraud-limit-00.txt **[0011]**
- *IETF's latest standard for Authentication, Authorization and Accounting - that for Diameter (RFC 3588),* 2003 **[0011]**