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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
1 April 2010 (01.04.2010)

PCT

(10) International Publication Number
WO 2010/034516 A1

(51) International Patent Classification:
*H04M 3/436* (2006.01) *H04L 12/58* (2006.01)
*H04L 29/06* (2006.01)

(21) International Application Number:
PCT/EP2009/006972

(22) International Filing Date:
28 September 2009 (28.09.2009)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
08017105.1 29 September 2008 (29.09.2008) EP

(71) Applicant *(for all designated States except US)*: **NEC EUROPE LTD.** [DE/DE]; Kurfuersten-Anlage 36, 69115 Heidelberg (DE).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: **D'HEUREUSE, Nico** [DE/DE]; Mannheimer Strasse 307, 69123 Heidelberg (DE). **TARTARELLI, Sandra** [IT/DE]; Hedwig-Kettler-Strasse 6, 76137 Karlsruhe (DE). **NICCOLINI, Saverio** [IT/DE]; Carl-Philipp-Fohr-Strasse 4, 69121 Heidelberg (DE).

(74) Agent: **SIEPE, André**; Ullrich & Naumann, Luisenstrasse 14, 69115 Heidelberg (DE).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

**Published**:

— *with international search report (Art. 21(3))*

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*

(54) **Title**: METHOD FOR IDENTIFYING DESIRED COMMUNICATION SESSIONS

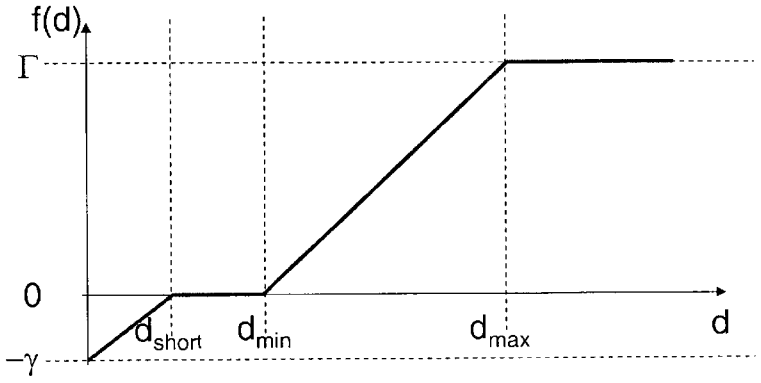


**Fig. 2**

(57) **Abstract**: A method for identifying desired and undesired SPIT/SPAM over IP communication sessions, in particular telephone calls, preferably in a VoIP network, in which users - callers - direct communication requests to other users - call recipients -, wherein said communication requests each get assigned a credit value indicating a level of trust said caller has towards said call recipient, is characterized in that the duration of past communication sessions between said caller and said call recipient is considered for determining the amount of said credit value, wherein said credit value only possesses mutual validity within the specific pair of users including said caller and said call recipient.

WO 2010/034516 A1

# METHOD FOR IDENTIFYING DESIRED COMMUNICATION SESSIONS

The invention relates to a method for desired communication sessions, in particular telephone calls, preferably in a VoIP network, in which users – callers – direct communication requests to other users – call recipients –, wherein said communication requests each get assigned a credit value indicating a level of trust said caller has towards said call recipient.

In the area of electronic mail unsolicited bulk email messages, so-called SPAM, have become very prevalent and have turned into a severe problem. Not only companies that require email communication are impacted by SPAM messages, but also private users are very annoyed by SPAM. Many Internet users nowadays receive more SPAM messages than regular emails. For this reason, almost every server for incoming email uses SPAM filters which check incoming mails according to defined rules. They search, for example, actively for key words in the content of an email, they check specific configurations of the server used for sending the email or they search for senders that are often used for sending bulk emails. In case of a matching classification of an email as SPAM, it is marked and/or sorted out.

In the area of – analog or digital – telephony, SPAM (in this context referred to as SPIT, SPam over Internet Telephony) also occurs more and more often, as it can be seen, for example, in case of undesired commercial or advertising calls. These calls are mostly made by automated calling machines. In the public switched telephone networks (PSTN), which today are still mainly employed, such SPAM calls are relatively expensive which is the reason for a rather restricted number of SPAM calls. Against the background of the rapid development of Internet telephony, also known as Voice over IP (VoIP), however, a massive increase of spam calls must be assumed since they are significantly simpler and more economical to realize in comparison to public switched telephone networks. The ultimate success of Internet telephony is therefore severely threatened by SPIT. Hence, processes for blocking SPIT are increasingly gaining interest and in the

future will probably reach an importance comparable to those processes which today are used for blocking e-mail spam.

The processes used in e-mail spam filters cannot, however, be transferred to telephony, or can only be transferred in part and in a very restricted manner. Thus, for example, the complete content of an e-mail is examined by a spam filter before the message is passed on to the recipient. A procedure of this type is not possible in the case of telephone conversations (or other forms of real-time or near real-time communication methods) since the content of a telephone conversation only becomes known in the course of the conversation.

Recently, research and standardization activities have tackled the SPIT issue and resulted in a number of methods that attempt to identify and possibly block/redirect SPIT calls or – equally important – to identify legitimate, i.e. non-SPIT, calls. Among these methods, social networks and global reputation systems have been pointed out as potentially useful techniques to assess the trustworthiness of a caller (as described, for instance, in V. A. Balasubramaniyan et al., "CallRank: Combating SPIT Using Call Duration, Social Networks and Global Reputation", in Proc. Fourth Conference on Email and Anti-Spam, August 2-3, 2007, Mountain View, California, USA; or in J. Rosenberg et al., "The Session Initiation Protocol (SIP) and Spam", RFC 5039, January 2008). These methods are typically based on user feedback that impacts the level of trust that each user enjoys within a group of users. The resulting reputation score is globally valid within the group of users (e.g. within a provider's network) and helps deciding whether a call should reach the call recipient (callee) or not. One of the main drawbacks of global reputation systems is, however, that they are complex to manage, in particular if the number of participating users is large. Further, they can suffer from artificially created positive reputation, e.g. when a number of malicious users or identities constitute a kind of "mafia" by giving a positive feedback to another malicious user.

Another drawback of the above mentioned "CallRank" solution is that it, if not deployed in a centralized manner, requires signaling to distribute credentials, which makes the system vulnerable to attacks. Further, it requires some changes to the signaling to include the credentials in the signaling messages, e.g. INVITE

messages, and to include some certification of the call length when a call finishes, e.g. in the BYE message. Moreover, it has inherent security issues as the approach bases on call credentials which have to be delivered within the network and therefore need to be protected by some mechanism, e.g., digital signatures. When deployed as a centralized solution, the "CallRank" solution does not scale for a large number of participating users.

It is therefore an object of the present invention to improve and further develop a method of the initially described type for identifying desired communication sessions in such a way that desired communication sessions can be ascertained in an efficient and reliable way while the management complexity of the desired call identification procedure is significantly reduced and malicious interactions are widely precluded.

In accordance with the invention, the aforementioned object is accomplished by a method comprising the features of claim 1. According to this claim such a method is characterized in that the duration of past communication sessions between said caller and said call recipient is considered for determining the amount of said credit value, wherein said credit value only possesses mutual validity within the specific pair of users including said caller and said call recipient.

According to the invention it has first been recognized that an identification of desired communication sessions on the basis of the duration of past communication sessions proves to be particularly reliable since it is nearly impossible to falsify or change this information with malicious intent. Accordingly, circumvention of the process is ruled out to the greatest possible extent. Furthermore, the method according to the invention effectively countermeasures SPIT by providing a very high degree of trustworthiness since the indication of whether a user A can be trusted by a user B, when A calls B, is evaluated on the basis of past communications between these two users only, i.e. on a solely mutual basis. This is in contrast to complex global reputation systems that consider user feedback within a group of users. Consequently, as the trust is based only on the mutual interactions between two users and does not have a

global validity for a group of users (e.g. within a provider's network) the method according to the invention is robust against so called "mafia" impacts.

When user A calls user B, the method according to the invention gives a reliable measure of the trustworthiness of user A towards user B. The level of trust is measured in credits. The higher the amount of credits that user A has collected towards user B (i.e. that "user A can present to user B") when A initiates a communication sessions with user B, the higher is the possibility that the communication sessions is accepted by user B, e.g. that a call reaches user B and is not considered to be SPIT to otherwise malicious or unsolicited. In other words, the level of trust that user A presents to user B, when A calls B, helps in deciding whether an incoming communication session is to be considered legitimate or not or to determine whether a call should be considered SPIT or not, i.e. whether the call should reach the recipient or not.

Besides its high trustworthiness and reliability the method according to the invention is characterized by a rather low complexity compared to existing reputations system. For instance, only a very limited number of data is to be stored, the parameter configuration is relatively easy and no changes in the signalling are required.

It is to be noted that the method provides a positive support for communication sessions between users that already have communicated with each other in the past, e.g. by established VoIP calls between each other. For users who "meet" each other for the first time, it may be provided that other methods are in place to assess the level of maliciousness of a call. After a first contact has been established, the method according to the invention can be applied for all subsequent communication sessions between that pair of users.

Moreover it is worth mentioning that the method according to the invention is independent of the protocol used for the signaling of the communication sessions. Thus, the method can be used with the protocol H.323, with SIP (Session Initiation Protocol), but also with protocols which will come into use in the future. Moreover, the method according to the invention requires no specific device as host.

In the framework of an advantageous embodiment a credit bucket $c_{BA}$ is set up for each ordered pair of users (A, B), wherein the credit bucket $c_{BA}$ is being updated for communication sessions directed from user A towards user B. This means that a further credit bucket $c_{AB}$ is set up which is related to the user pair including users A and B and which is being updated for calls in the reverse direction, i.e. for communication sessions directed from user B towards user A. As will be explained in more detail below, for asserting the trustworthiness of a session directed from user A to user B, both credit buckets $c_{AB}$ and $c_{BA}$ are considered whereby higher priority should be given to the current value of $c_{AB}$. By means of credit buckets the dynamics of the credits that are a measure of the level of trust can be effectively ruled and tracked.

With respect to obtaining trust towards another user it may be provided that the credit bucket $c_{BA}$ is filled with a certain amount of credits in case the duration of a communication session directed from user A towards user B is longer than a configurable threshold. On the other hand it may be provided that the credit bucket $c_{BA}$ is emptied by a certain amount of credits in case the duration of a communication session directed from user A towards user B is shorter than a second configurable threshold. However, in case user A had not yet obtained any credits towards user B, the credit bucket $c_{BA}$ does not need to be updated (emptied). Such filling and emptying strategy would reflect a typical telephony behavior in which a user will normally terminate a call rather promptly in case he realizes that the call is e.g. an undesired machine generated advertising call, whereas a call with e.g. a (trusted) friend might take some time.

According to a preferred embodiment credit bucket $c_{BA}$ is gradually emptied after a configurable time period has lapsed since the last communication session directed from user A towards user B. Insofar, the credit bucket are designed as "leaky" credit buckets. The decrease of the credit level may follow, e.g., a linear function or an exponential function.

With respect to user-friendliness and a high degree of individual flexibility it may be provided that the configuration parameters for filling/emptying the credit bucket $c_{BA}$,

in particular the above mentioned thresholds, can be specified by user A. Consequently, a user can treat other users individually, for instance he can specify that the credit of a user B shall decrease linearly after only two days have lapsed since he last called user B, whereas the credit of another user C shall decrease exponentially not until after one month has lapsed since he last called that user C.

Regarding a comprehensive consideration with respect to the trust evaluation, in a preferred embodiment the amount of the credit value that a caller A has towards a call recipient B is evaluated as a function of the current level of both credit buckets $c_{AB}$ and $c_{BA}$. This means that both the communication sessions directed from user A towards user B as well as the communication sessions of the opposite direction are taken into consideration for the trust evaluation. However, advantageously the credit bucket $c_{AB}$ (that depends on past communication sessions initiated by user B towards user A) will be given the higher impact in the evaluation of the amount of said credit value that a caller A has towards a call recipient B.

According to a further preferred embodiment the function for calculating the amount of the credit value that a caller A has towards a call recipient B will be designed in such a way that the amount of the credit value is zero in case that user B has never directed a communication request to user A in the past. Consequently, it will be particularly difficult for a malicious user, e.g. a machine automatically generating advertisement calls, to gain credibility towards another user since it is very unlikely that this user will have directed any communication sessions towards the malicious user.

With respect to proper implementation allowing for efficient functionality it may be provided that the credit buckets are managed centrally by a network entity that, for instance in cases of VoIP communications, calls typically have to pass on their way to the call recipient. In particular, the network entities hosting the credit buckets management together with the trust evaluation functionality may include, but not limited to, a network border element (such as a Session Border Controller, SBC), a proxy server, an application server and/or a gatekeeper.

Alternatively, a decentralized solution may be implemented. In such case the credit buckets as well as the calculation of the amount of the credit value a caller has towards a call recipient would be managed locally by the users' communication devices. In this context it is important to note that it is not necessary that both communication devices of a pair of users support the required functionality. Even if the caller's (or the call recipient's) communication device is not enabled to carry out the method according to the invention, it would still be possible for the other party (that has respective support) to implement and use the method.

Advantageously, the parameters being stored for each ordered user pair (A, B) include the last time user A directed a communication request to user B, the last time user B directed a communication request to user A, and the actual level of said credit buckets $c_{BA}$ and $c_{AB}$. Consequently, only a very low number of variables is stored, making the method easy to implement without requiring any extensive resources.

Besides telephone calls via VoIP, which are intended to constitute the main application field of the present invention, it may also be provided that the communication sessions include other kinds of communications that are protected, for example instant messaging (IM) sessions. In addition to the duration of past sessions the number of words and/or the number of characters exchanged within a messaging session may be considered for determining the amount of the credit value between a caller and a call recipient. Moreover, the duration between first and last message, the number of messages exchanged or similar parameters may be taken into consideration. According to one embodiment the level of trust might depend only on the past communication between two users using the specific technology (e.g. protect instant messaging based on the past mutual instant messaging activity). According to an alternative embodiment aiming at an optimized overall performance the past history of other applications, in particular the past mutual telephone activity, may be considered for the determination of the amount of the credit value between IM caller and IM call recipient (e.g. protect instant messaging based on the past mutual instant messaging activity as well as on the mutual telephone activity).

There are several ways how to design and further develop the teaching of the present invention in an advantageous way. To this end, it is to be referred to the patent claims subordinate to patent claim 1 on the one hand, and to the following explanation of a preferred example of an embodiment of the invention illustrated by the drawing on the other hand. In connection with the explanation of the preferred example of an embodiment of the invention by the aid of the drawing, generally preferred embodiments and further developments of the teaching will be explained. In the drawings

Fig. 1 schematically illustrates a credit bucket according to an embodiment of the present invention,

Fig. 2 illustrates the time dependency of a credit bucket filling function according to an embodiment of the present invention, and

Fig. 3 illustrates the time dependency of a credit bucket exhaustion function according to an embodiment of the present invention.

FIG. 1 shows, schematically, an embodiment example of the method according to the invention for identifying desired calls that provides a strong indication of whether user A can be trusted by user B, when A calls B. Contrary to complex global reputation systems, the trustworthiness of user A towards user B depends on past VoIP communications between A and B only. The level of trust that A presents to B, when A calls B increases with the duration of the previous conversations between A and B, provided that calls are longer then a minimum duration. Conversely, calls with very short durations, below a configurable threshold, contribute to the trust level with a negative score. Moreover, the level of trust decreases with the time elapsed since B last called A. The level of trust is measured by means of credits. The dynamics of the credits are rules by mean of a bucket.

In the embodiment illustrated in Fig. 1 it is assumed that for each ordered user pair (A, B) a credit bucket is set up from which a measure of trust a caller A has towards a call recipient B can be evaluated. When A calls B, then the credit bucket $c_{BA}$ is considered, when B calls A the credit bucket $c_{AB}$ is considered. For the sake of simplicity, in Fig. 1 only credit bucket $c_{BA}$ is depicted, however, the following explanations apply for the credit bucket $c_{AB}$ in the same way.

The credit buckets are filled according to a function $f(d)$, where $d$ is the duration of the call. The illustrated bucket level of $c_{BA}$ at time $n$ is referred to as $c_{BA,n}$, which increases every time A calls B and the call is long enough. Moreover, the credit bucket $c_{BA}$ is emptied according to a function $e(\Delta t)$, where $\Delta t$ is the time elapsed since last time A called B.

When A calls B, the credit that A presents to B (i.e. the credit user A has collected with respect to user B) is evaluated as a function of both bucket levels $c_{BA,n}$ and $c_{AB,n}$, however $c_{AB,n}$ has the higher impact, as will be explained in more detail below. When A calls B, at the beginning of the call first the new bucket level $c_{BA,n}$ is evaluated based on the time elapsed since the last time A called B, i.e. based on the function $e(\Delta t)$ that will be discussed in connection with Fig. 3. Then a temporary bucket level $\chi_{AB,n}$ is evaluated based on the time elapsed since the last time B called A, i.e. based on function $e(\Delta t)$. The actual update of the bucket level $c_{AB,n}$ happens only when B calls A, so that the reference time for $\Delta t$ is always last time B called A. Insofar, the variable $\chi_{AB,n}$ represents a kind of snapshot only with no database update. Finally, the credits that A presents to B are evaluated as:

$$cred_{AB,n} = \alpha^{*}\chi_{AB,n}+(1-\alpha)^{*}\chi_{AB,n}{}^{*}c_{BA,n}$$

The rationale is that, when A calls B, in order for A to present the highest credits to B, a) user B must have called A so that bucket $c_{AB}$ is full, and b) user A must also have called user B so that $c_{BA}$ is full. Besides, if B has never called A in the past, then $c_{AB}$ is zero (therefore also $\chi_{AB,n}$ is zero) and the total credits $cred_{AB,n}$ will also be evaluated to zero.

When the call ends the bucket level $c_{BA,n}$ is updated based on the duration of the call, i.e. based on the function *f(d)* that will be discussed in connection with Fig. 2.

The above credits can be used to evaluate a score within a more complex SPIT prevention system. The score is a measure of how likely it is that a call is SPIT or otherwise unsolicited. A negative score will correspond to a certain level of suspiciousness, that the call is SPIT or otherwise unsolicited. The score resulting from the proposed crediting system can be evaluated as $score_n = cred_{AB,n}/C$, where $C$ is the depth of the credit buckets.

Fig. 2 illustrates the time dependency of the credit bucket filling function *f(d)* according to an embodiment of the present invention. Basically, the amount of credits grows with the time users A and B communicated with each other in the past using telephony, provided that the calls reach a minimum call duration. Conversely, if calls are shorter than a configurable threshold, the amount of credits will be decreased. In particular, when A calls B: If the call is longer than a configurable threshold $d_{min}$, then B obtains a certain amount of credits towards A. Calls being longer than a configurable threshold $d_{max}$ all receive the maximum credit $\Gamma$, wherein $\Gamma < C$, so that one single call cannot fill up the credit bucket completely. If a call is shorter than a configurable threshold $d_{short}$, then B loses a small amount of credits (provided that B had already credits towards A, otherwise nothing happens). The same procedure is applied for credit bucket $c_{AB}$ if B calls A

When A calls B, at the end of the call $c_{BA,n}$ is evaluated as

$$c_{BA,n} = max\,[0,\ min[C,\ c_{BA,n-1} + f(d)]]$$

The function *f(d)* can be expressed in formula as:

$$f(d) = \begin{cases} \frac{\gamma}{d_{short}} * d - \gamma & 0 < d < d_{short} \\ 0 & d_{short} < d < d_{\min} \\ \frac{\Gamma}{d_{\max} - d_{\min}}(d - d_{\min}) & d_{\min} < d < d_{\max} \\ \Gamma & d > d_{\max} \end{cases}$$

Alternatively, the following formulation for *f(d)* can be used:

$$f(d) = \begin{cases} -\gamma & 0 < d < d_{short} \\ 0 & d_{short} < d < d_{\min} \\ \dfrac{\Gamma}{d_{\max} - d_{\min}}(d - d_{\min}) & d_{\min} < d < d_{\max} \\ \Gamma & d > d_{\max} \end{cases}$$

Fig. 3 illustrates the time dependency of the credit bucket exhaustion function *e(Δt)*, which determines the way the credit bucket is emptied. If the bucket level $c_{BA}$ is considered, then $\Delta t$ is the time difference between the actual time and last time A called B. If no call is established from A to B for at least $\Delta t_{min}$ then B starts losing credits, i.e. $c_{BA}$ is reduced. If no call is established from A to B for at least $\Delta t_{max}$ then B loses all credits, i.e. $c_{BA}$ is completely emptied (*C* is the depth of the credits bucket).

The credits bucket level at time *n* is evaluated as:

$$c_{BA,n} = max\,[0,\ c_{BA,n-1} - e(\Delta t_n)]$$

where (n-1) is the last time the bucket level was updated. Equivalently, the temporary value $\chi_{BA,n}$ is evaluated as:

$$\chi_{BA,n} = max\,[0,\ c_{BA,n-1} - e(\Delta t_n)]$$

where (n-1) is the last time the bucket level was updated.

The function *e(Δt)* can be expressed in formula as:

$$e(\Delta t) = \begin{cases} 0 & 0 < \Delta t < \Delta t_{\min} \\ \dfrac{C}{\Delta t_{\max} - \Delta t_{\min}}(\Delta t - \Delta t_{\min}) & \Delta t > \Delta t_{\min} \end{cases}$$

As becomes clear from the above, the method according to the present invention works with a low number of variables being stored, thus no excess storage capabilities are required. For each ordered user pair (A, B), for which user A and B communicated with each in the past other, e.g. using VoIP, the following parameters will be kept updated and will be stored:

- last time A called B
- last time B called A
- credit bucket levels $c_{AB,n}$ and $c_{BA,n}$

A bucket entry $c_{AB}$ for the user pair (A, B) can be removed from memory every time that the temporary value of the bucket occupation $\chi_{AB,n}$ is evaluated zero. This can happen either when A calls B or through a clean up process that regularly checks for outdated entries. It is to be noted that if A calls B at time *n* and no bucket is allocated for the user pair (A,B), then only bucket $C_{BA}$ will be updated/created, but $C_{BA}$ does not need being allocated (simply use $cred_{AB,n} = 0$).

The following parameters are variables that can be configured either centrally by a network entity or in a decentralized manner by the users' individual communication devices:

- credit bucket depth *C*
- $\alpha$ i.e. the weight to be given to the credit that B presents to A when A calls B
- $\Delta t_{min}$ and $\Delta t_{max}$ for the function $e(\Delta t)$
- $d_{short}$, $d_{min}$, $d_{max}$, $\gamma$ and $\Gamma$ for the function $f(d)$.

An example of reasonable configuration values could be as follows:

- $C = 1$
- $\alpha = 0.9$
- $\Delta t_{min}$ = 1 week and $\Delta t_{max}$ = 1 month
- $d_{short}$ = 15 sec, $d_{min}$ = 30 sec, $d_{max}$ = 180 sec
- $\gamma = 0.05$, $\Gamma = 0.8$

With the above values, for A to achieve a full credit bucket $c_{AB}$ at step n (i.e. $c_{AB,n}=1$), user B must call A at least twice,

e.g. one long call of at least 3 minutes and a shorter one of about 1 minute within one week, or

e.g. 6 times for about 1 minute within one week.

Many modifications and other embodiments of the invention set forth herein will come to mind the one skilled in the art to which the invention pertains having the benefit of the teachings presented in the foregoing description and the associated drawings. Therefore, it is to be understood that the invention is not to be limited to the specific embodiments disclosed and that modifications and other embodiments are intended to be included within the scope of the appended claims. Although specific terms are employed herein, they are used in a generic and descriptive sense only and not for purposes of limitation.

# Claims

1. Method for identifying desired communication sessions, in particular telephone calls, preferably in a VoIP network, in which users – callers – direct communication requests to other users – call recipients –, wherein said communication requests each get assigned a credit value indicating a level of trust said caller has towards said call recipient,
characterized in that the duration of past communication sessions between said caller and said call recipient is considered for determining the amount of said credit value, wherein said credit value only possesses mutual validity within the specific pair of users including said caller and said call recipient.

2. Method according to claim 1, wherein a credit bucket $c_{BA}$ is set up for each ordered pair of users (A, B), wherein said credit bucket $c_{BA}$ is being considered for communication sessions directed from user A towards user B.

3. Method according to claim 2, wherein said credit bucket $c_{BA}$ is filled with a certain amount of credits in case the duration of a communication session directed from user A towards user B is longer than a first configurable threshold.

4. Method according to claim 2 or 3, wherein said credit bucket $c_{BA}$ is emptied by a certain amount of credits in case the duration of a communication session directed from user A towards user B is shorter than a second configurable threshold.

5. Method according to any of claims 2 to 4, wherein said credit bucket $c_{BA}$ is gradually emptied after a configurable time period has lapsed since the last communication session directed from user A towards user B.

6. Method according to any of claims 3 to 5, wherein configuration parameters for filling/emptying said credit bucket $c_{BA}$, in particular said first and said second thresholds, are specified by said user A.

7. Method according to any of claims 2 to 6, wherein the amount of said credit value that a caller A has towards a call recipient B is evaluated as a function of the current level of both said credit buckets $c_{AB}$ and $c_{BA}$.

8. Method according to claim 7, wherein said credit bucket $c_{AB}$ has the higher impact in the evaluation of the amount of said credit value that a caller A has towards a call recipient B.

9. Method according to any of claims 2 to 8, wherein the amount of said credit value that a caller A has towards a call recipient B is zero in case that user B has never directed a communication request to user A in the past.

10. Method according to any of claims 2 to 9, wherein said credit buckets are managed centrally by a network entity, in particular by a network border element, a proxy server, an application server and/or a gatekeeper.

11. Method according to any of claims 2 to 9, wherein said credit buckets are managed locally by said users' communication devices.

12. Method according to any of claims 2 to 11, wherein the parameters being stored for each ordered user pair (A, B) include the last time user A directed a communication request to user B, the last time user B directed a communication request to user A, and the actual level of said credit buckets $c_{BA}$ and $c_{AB}$.

13. Method according to any of claims 1 to 12, wherein said communication sessions include instant messaging sessions.

14. Method according to claim 13, wherein the number of words and/or characters exchanged within a messaging session is considered for determining the amount of said credit value between said caller and said call recipient.

15. Method according to claim 13 or 14, wherein the past history of other applications, in particular the past mutual telephone activity, is considered for the

determination of the amount of said credit value between said caller and said call recipient.

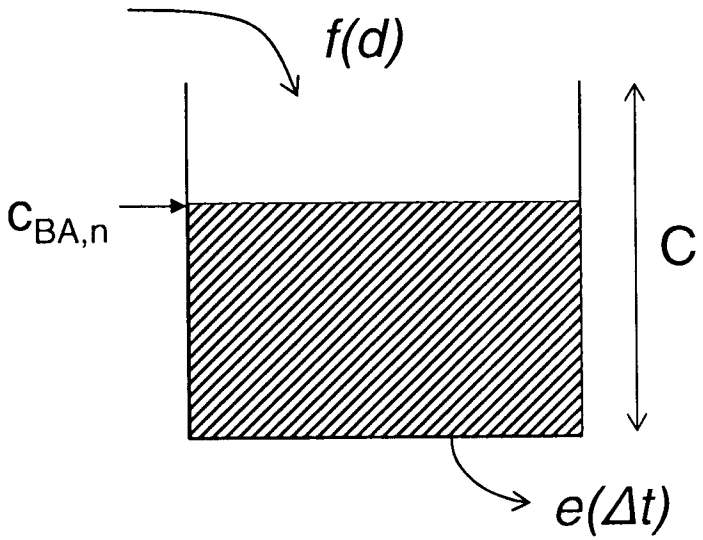


Fig. 1

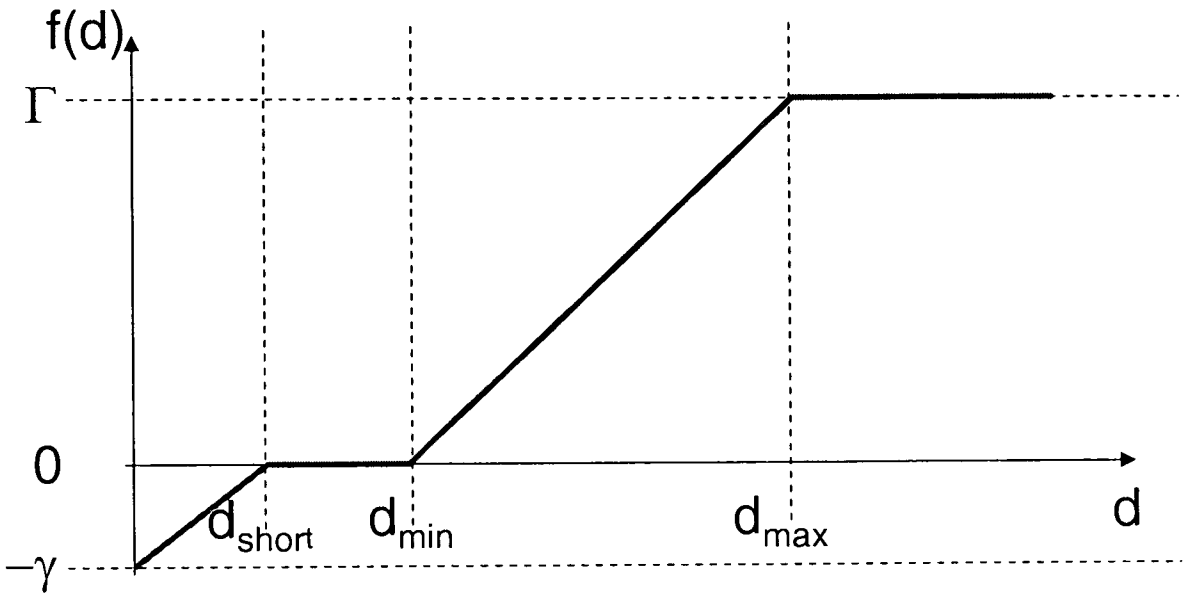


Fig. 2

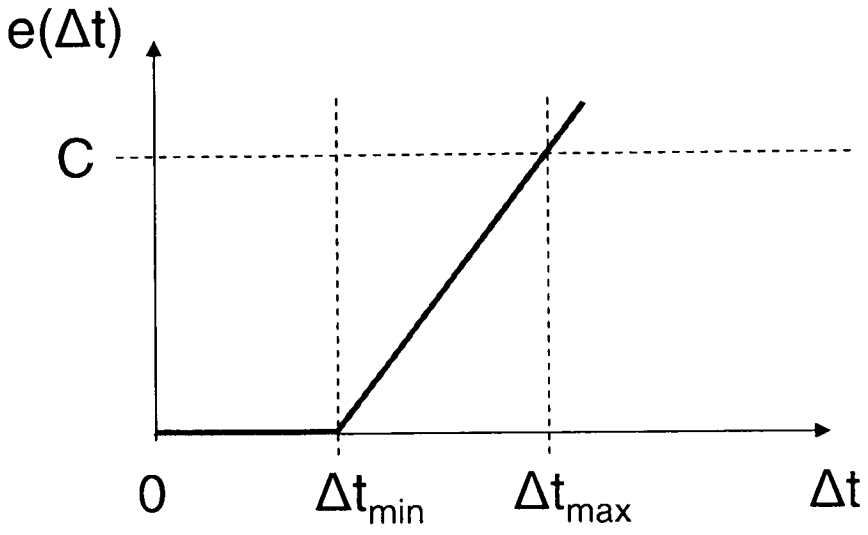


Fig. 3

# INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2009/006972

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04M3/436 H04L29/06 H04L12/58

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)
H04M H04L

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

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| X | WO 2007/030951 A1 (EYEBALL NETWORKS INC [CA]; PICHE CHRISTOPHER [CA]; KHAN SHAHADAT [CA];) 22 March 2007 (2007-03-22) page 11, line 17 - page 14, line 16 figure 4 | 1-15 |
| X | Vijay A. Balasubramaniyan, Mustaque Ahamad, Haesun Park: "CallRank: Combating SPIT Using Call Duration, Social. Networks and Global Reputation" 3 August 2007 (2007-08-03), XP002565207 Retrieved from the Internet: URL:http://www.ceas.cc/2007/papers/paper-63.pdf> [retrieved on 2010-01-20] the whole document | 1-15 |

☐ 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

"E" earlier document 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 January 2010 | 08/02/2010 |

| Name and mailing address of the ISA/ | Authorized officer |
|---|---|
| European Patent Office, P.B. 5818 Patentlaan 2<br>NL - 2280 HV Rijswijk<br>Tel. (+31-70) 340-2040,<br>Fax: (+31-70) 340-3016 | Nash, Michael |

# INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2009/006972

| Patent document cited in search report | Publication date | Patent family member(s) | Publication date |
|---|---|---|---|
| WO 2007030951 A1 | 22-03-2007 | CA 2622821 A1 | 22-03-2007 |
| | | CN 101310489 A | 19-11-2008 |
| | | KR 20080065974 A | 15-07-2008 |