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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
12 April 2007 (12.04.2007)

PCT

(10) International Publication Number
WO 2007/041157 A1

(51) International Patent Classification:
H04L 12/28 (2006.01) *H04L 29/06* (2006.01)

(21) International Application Number:
PCT/US2006/037658

(22) International Filing Date:
27 September 2006 (27.09.2006)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
11/242,397 3 October 2005 (03.10.2005) US

(71) Applicant *(for all designated States except US)*: **LUCENT TECHNOLOGIES INC.** [US/US]; 600 Mountain Avenue, Murray Hill, NJ 07974-0636 (US).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **GLINKA, Michael, Frank** [DE/DE]; Hiltpolsteiner Str. 3, 90411 Nuremberg (DE).

(74) Agent: **FINSTON, Martin, I.**; LUCENT TECHNOLOGIES INC., Docket Administrator- Room 3J-219, 101 Crawfords Corner Road, Holmdel, NJ 07733 (US).

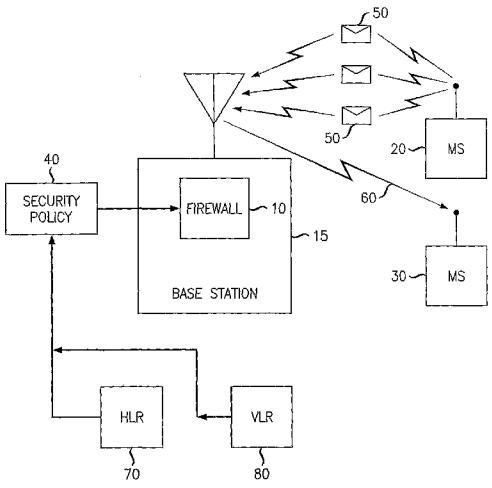
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, 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, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

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:** WIRELESS NETWORK PROTECTION AGAINST MALICIOUS TRANSMISSIONS



(57) **Abstract:** A method and apparatus are provided for protecting a wireless network from malicious code transmitted from a user terminal. Traffic from user terminals which flows over the air-interface is filtered and evaluated according to a set of rules imposed by the network, or specified by the user, or both. If the evaluation indicates that the traffic is offensive, further traffic from the offending user is blocked, and optionally, the offense is reported. As a consequence, a user can be protected from unwanted traffic that has been destined to terminate on his mobile, and protected from having his own mobile make undesired transmissions.

WO 2007/041157 A1

WIRELESS NETWORK PROTECTION AGAINST MALICIOUS TRANSMISSIONS

Field of the Invention

This invention relates to security in wireless communication networks.

Art Background

It has become commonplace to use mobile phones for making voice calls or for sending messages via a SMS service. Recently, however, the mobile phone market has seen the introduction of smartphones. These devices incorporate at least some of the functionality of personal computers. As a consequence, they can, among other things, run software programs, receive email, make automatic calls, maintain open internet connections, browse the Web, and act under remote control.
It is well known that personal computers are vulnerable to viruses, Trojan horse programs, and other forms of malicious code, and can propagate such code over the communication networks to which they are attached. With the expanded computational functionality of mobile phones, they, too, can suffer damage from malicious code and can propagate it over the wireless network. A mobile communication device or other user terminal may become infected, for example, over the air interface, or from a bluetooth, WiFi, or infrared connection.

This threat has been recognized. In response, antivirus programs have been made available for protecting mobile communication devices such as smartphones. However, these products fail to address the threat to the wireless network from malicious code that might be transmitted on the uplink from a mobile device or other user terminal.

Summary of the Invention

I have found a way to protect the wireless network from malicious code transmitted from a user terminal. In accordance with my development, traffic from user terminals which flows over the air-interface is filtered and evaluated according to a set of rules imposed by the network, or specified by the user, or both. If the

evaluation indicates that the traffic is offensive, further traffic from the offending user is blocked, and optionally, the offense is reported. As a consequence, a user can be protected from unwanted traffic that has been destined to terminate on his mobile, and protected from having his own mobile make undesired transmissions.

Brief Description of the Drawing

FIG. 1 is a high-level conceptual drawing of a portion of a wireless network, including a base station equipped with a firewall as described herein.

Detailed Description

The methods to be described below can be applied independently of any specific wireless technology such as UMTS, CDMA, or GSM. Moreover, they can be applied in respect of any fixed or mobile user served by the network, independently of the type of operating system and user terminal.

For purposes of illustration, the user terminal will often be referred to, below, as a "mobile terminal." However, this choice of terminology is not meant to be limiting. It will be understood that the same methods apply to any other type of user terminal, including fixed terminals, and that the scope of the invention is not limited to a terminal of any particular sort.

One attack route for malicious code is via the Short Messaging System (SMS) if available on the network. SMS messages are normally processed (depending on whether the technology is, e.g., GSM, UMTS, or CDMA) by a SMS message center. Protection against unwanted messages launched by malicious code can be provided by a filter implemented as a SMS/MMS firewall. Such a firewall is advantageously installed at the earliest feasible processing stage in the network. With reference to FIG. 1, for example, it would be advantageous to implement firewall 10 at base station 15 (or, e.g., a Node B of a UMTS network) at the level directly following the air interface.

Such a solution could also be effective to block virulent mass traffic to and from mobiles within the core network. Advantageously, such a solution will protect a user 20, 30 from unwanted traffic that has been destined to terminate on his mobile, and will protect the user from having his own mobile make undesired transmissions.

One type of rule that could be implemented by the SMS/MMS firewall would relate to the number of SMS messages sent by a mobile within a specified time frame. That is, the user, e.g., causes a security policy 40 to be applied. The security policy includes a maximum number of SMS messages 50 that may be sent by the mobile within a specified length of time. If this number of messages is exceeded, the firewall causes the mobile to be blocked. Optionally, a notification may be sent to the user, informing him that his mobile is behaving in an unauthorized or virulent manner.

More specifically, the firewall or filter at the base station counts the number of, e.g., SMS transmissions, MMS transmissions, calls, or data connections received in a given time frame. If the number exceeds the user's previously defined threshold or otherwise violates his applied security policy, then all traffic of this mobile will be directly blocked and the mobile user may be paged with a message notifying him that his mobile is behaving in a virulent matter. However, a predefined "white list" of permitted connections, such as emergency numbers, may still be permitted.

Another type of rule can apply a blacklist of numbers, maintained at the Node B (more generally, the "base station") and updated by the operator, that are prohibited from connecting with the mobile. Blacklisted and blocked numbers may include, e.g., telephone numbers, Web pages, email addresses, and data connections. For updating of blacklists, fraudulent or malicious cases may be reported to a central database at, e.g., the HLR 70 and VLR 80, as well as reported to the mobile user. To exclude blacklisted calls, the firewall or filter may, e.g., monitor not only calls transmitted from the mobile, but also calls to be transmitted over the air interface to the mobile. (At least some blacklisted calls may be excluded as a result of monitoring the call set-up messages. In this regard, it may in at least some cases be sufficient to monitor only those set-up messages transmitted from the mobile.)

A user may have a personal filter configured according to his own security policy. Generally, the user will wish to prevent virulent behavior by his own mobile, and to be protected from being charged for the use of expensive services 60 which were invoked without his knowledge or consent. If the user leaves the filter unconfigured, or specifies that the security policy should be inactive, the user will experience normal, unprotected network behavior.

Part of the policy defined by the user may be an explicit exclusion of certain services. For example, the user explicity says, in effect, "I do not want E-bay pages to be accessed by my mobile until further notice." (E-bay, of course, is only one example of many types of services that might be excluded in this regard.)

The service provider may also administer a security policy, which may be additional to that defined by the user, and which may be subject to the user's consent. A network security policy may, for example, provide enhanced protection against present and future types of malicious code attacks. In particular, the network provider can provide a list that updates the base stations with known malicious connections.

Through its security policy, the network may also protect itself from being overloaded by massive amounts of irrelevant traffic. Such an undesirable scenario might arise, for example, if a virus causes a large group of mobiles to generate undesired SMS or MMS traffic all at the same time.

In this regard, it may be useful in some cases to add a filter or firewall as described above to enhance the security of a base station that covers a building, office park, stadium, or other area where there is a concentration of fixed or temporarily non-mobile users. The enhanced security may be useful, for example, to deter the type of attack scenario in which malicious code causes the concentrated user terminals to overwhelm the serving cell with traffic generated all at the same time.

It will be advantageous to a mobile user for the security policy to continue to apply after handover so that a moving user can experience uninterrupted protection. This can be achieved if, for example, a count of (potentially virulent) received calls (including, e.g., SMS, MMS, or data connections) is maintained not only at the base station, but also at the next network instance, such as the base station controller or RNC.

In general, when a call is made to a mobile terminal, the network will identify the called mobile and the location of the called mobile. Thus, those mobiles that have already been identified as virulent and for that reason have been blocked, can remain in "blocked" status until, e.g., the user sends a clearance message, or (in an emergency, for example) switches off his personal firewall.

It will be understood that various formats and protocols may be used for the exchange of control messages needed for implementation of the filter and security policy.

For example, control messages may be exchanged using normal traffic channels or, e.g., unused bandwidth or unused slots of control messages of other types.

In some cases, a user might wish to generate mass traffic, i.e., a large number of similar short messages within a short time period. For example, the user might wish to send meeting invitations to all the addresses on a long list of possible participants. Such mass traffic would be benign and not virulent. To permit such traffic to pass through the firewall, the user could, for example, send a notice to the firewall announcing that he will—immediately or within a specified time frame—send a mass SMS or other type of transmission.

Claims

What is claimed is:

1. A method for suppressing unwanted traffic in a wireless communication network, comprising:

at a base station (15), applying a security policy (40) to call traffic (50) received by the base station from a user terminal (20), thereby to determine whether the call traffic is undesirable; and

if the call traffic is determined to be undesirable, blocking at least some further call traffic from the user terminal.

2. The method of claim 1, wherein the step of applying a security policy comprises counting a number of calls sent within a time interval, and comparing the number with a threshold.

3. The method of claim 1, wherein the step of applying a security policy comprises determining whether the user terminal is sending an excessive number of SMS messages.

4. The method of claim 1, wherein the step of applying a security policy comprises comparing requested connections against a list of prohibited connections, and the blocking step comprises blocking connection if they are found on the list.

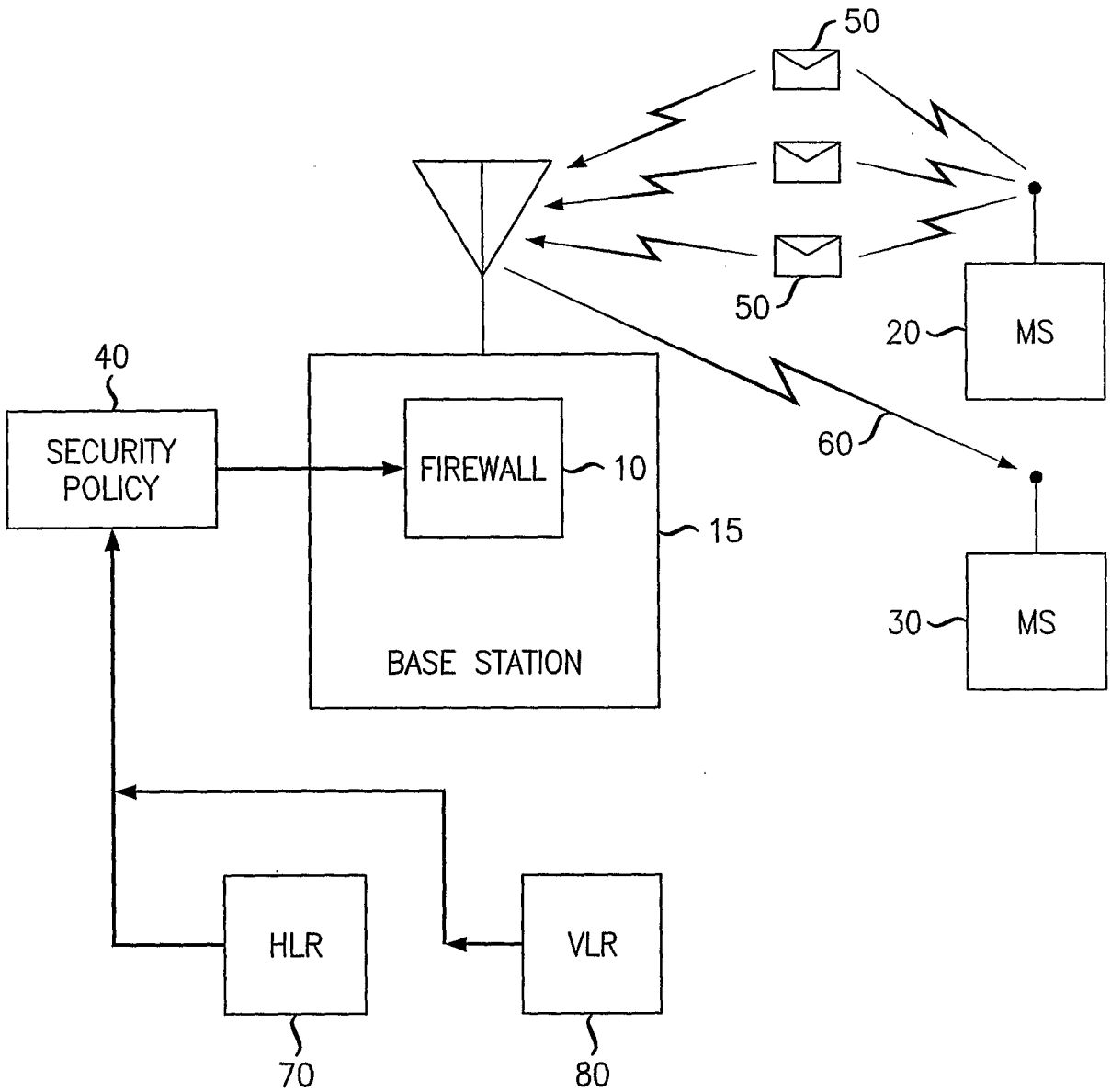
5. A security system at a base station (15) of a wireless communication network, comprising:

a circuit adapted to measure call volume per a time interval from individual user terminals and to indicate if said volume exceeds a threshold; and

a circuit adapted to respond to said indications by blocking at least some further traffic from the user terminal in respect to which said indications have been made.

6. The security system of claim 5, further comprising a database of prohibited connections and a circuit adapted to indicate if a prohibited connection is being

attempted, and wherein the blocking circuit is further adapted to block said attempts to make prohibited connections.


50
50
20
MS
40
SECURITY POLICY
FIREWALL
10
15
60
30
MS
BASE STATION
HLR
VLR
70
80

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2006/037658

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L12/28 H04L29/06

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)
H04L H04Q

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	US 2002/166068 A1 (KILGORE BRIAN [US]) 7 November 2002 (2002-11-07)	1,4
Y	paragraph 0010; paragraphs 0025-0026; paragraphs 0030-0031; paragraphs 0034-0036; paragraph 0041 --- -/--	2,3,6

[X] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier 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
30 January 2007	06/02/2007

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	MORENO-SOLANA, S

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2006/037658

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y	WO 03/055148 A (ESPHION LTD [NZ]; BRENDEL JUERGEN [NZ]) 3 July 2003 (2003-07-03) page 2, line 1 - line 18 page 3, line 6 - line 15 page 4, line 3 - line 8 page 5, line 1 - page 6, line 9 page 7, line 27 - page 8, line 3 page 10, line 24 - line 27 page 11, line 17 - line 20 page 14, line 3 - page 16, line 20 page 21, line 15 - line 32 page 22, line 19 - line 24 figure 3	5 2,3,6
A	US 2005/021740 A1 (BAR ANAT BREMLER [IL] ET AL) 27 January 2005 (2005-01-27) paragraphs 0010-0015; paragraphs 0032-0035; paragraph 0042; paragraph 0059; paragraph 0064; paragraphs 0069-0087 figures 2,3	1-6
A	WO 2004/097584 A2 (P G I SOLUTIONS LLC [US]) 11 November 2004 (2004-11-11) abstract paragraph 0065; paragraphs 0074-0076; paragraph 0089; paragraphs 0092-0094	1-6
A	WO 03/050644 A2 (RIVERHEAD NETWORKS INC [US]; AFEK YEHUDA [IL]; ZADIKARIO RAFI [IL]; TO) 19 June 2003 (2003-06-19) page 1, line 15 - page 4, line 11 page 5, line 3 - page 7, line 11 page 14, line 1 - page 15, line 15	1-6

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2006/037658

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2002166068 A1	07-11-2002	US 2006272013 A1	30-11-2006
WO 03055148 A	03-07-2003	AU 2002358361 A1	09-07-2003
		NZ 516346 A	24-09-2004
		US 2005125195 A1	09-06-2005
US 2005021740 A1	27-01-2005	WO 2004070509 A2	19-08-2004
WO 2004097584 A2	11-11-2004	NONE	
WO 03050644 A2	19-06-2003	NONE	