

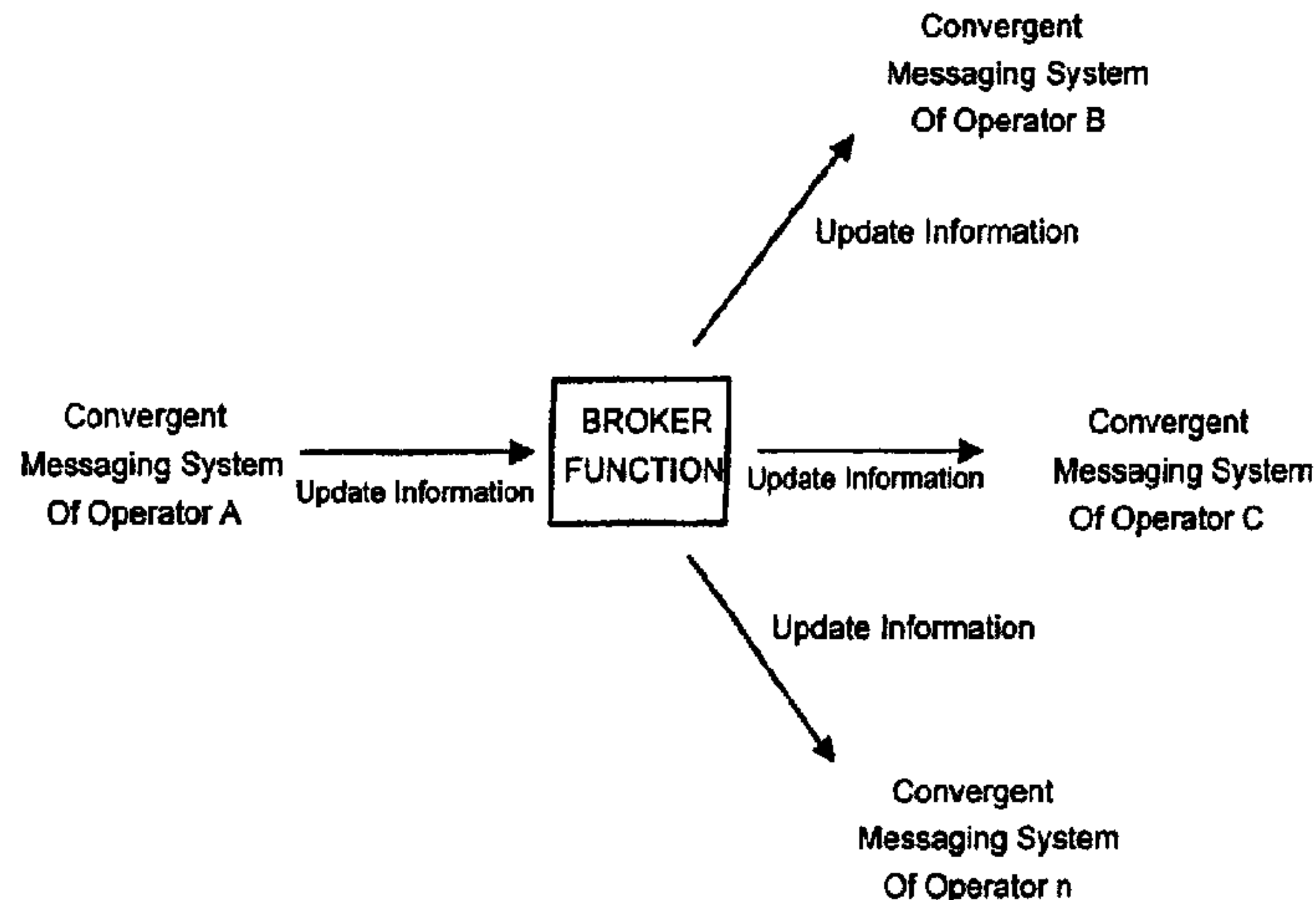


(86) Date de dépôt PCT/PCT Filing Date: 2008/09/13
(87) Date publication PCT/PCT Publication Date: 2009/04/09
(45) Date de délivrance/Issue Date: 2017/05/09
(85) Entrée phase nationale/National Entry: 2010/03/25
(86) N° demande PCT/PCT Application No.: EP 2008/007582
(87) N° publication PCT/PCT Publication No.: 2009/043435
(30) Priorité/Priority: 2007/09/26 (DE01 2007 045 909.4)

(51) Cl.Int./Int.Cl. *H04L 29/06* (2006.01),
H04W 12/12 (2009.01)
(72) Inventeur/Inventor:
ROEBKE, MATTHIAS, DE
(73) Propriétaire/Owner:
T-MOBILE INTERNATIONAL AG, DE
(74) Agent: MARKS & CLERK

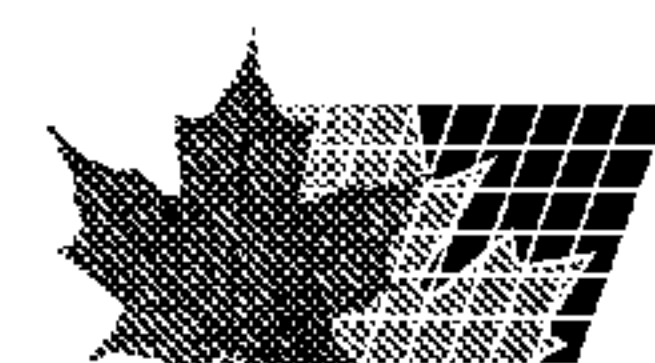
(54) Titre : PROCEDE ANTIVIRUS/SPAM DANS DES RESEAUX RADIOMOBILES

(54) Title: PROCESS TO PROTECT AGAINST VIRUSES/SPAM IN MOBILE BROADCAST NETWORKS



(57) Abrégé/Abstract:

The invention concerns a process to protect against viruses / spam in mobile broadcast networks containing convergent messaging services with transmission of protocol data, characterized by having functions included in the protocol of the convergent messaging service, which facilitate the exchange of virus / spam information between the network components of one or more network operators. The invention has the objective of providing a process for convergent messaging systems that will facilitate the exchange of information regarding viruses and spam across network and platform boundaries in order to combat their widespread dissemination.



Summary

The invention concerns a process to protect against viruses / spam in mobile broadcast networks containing convergent messaging services with transmission of protocol data, characterized by having functions included in the protocol of the convergent messaging service, which facilitate the exchange of virus / spam information between the network components of one or more network operators. The invention has the objective of providing a process for convergent messaging systems that will facilitate the exchange of information regarding viruses and spam across network and platform boundaries in order to combat their widespread dissemination.

Process to Protect against Viruses / Spam in Mobile Broadcast Networks

The invention concerns a process to protect against viruses / spam in mobile broadcast networks with convergent messaging services, which are undergoing standardization by the "Open Mobile Alliance".

Computer viruses and spam (the massive transmission of messages not desired by the recipient, such as advertising) are turning into increasingly significant problems in current computer networks, such as the Internet. Operators of e-mail services or Internet service providers attempt to combat this problem by resorting to local solutions.

It may be assumed that a similar problem will also emerge increasingly in mobile broadcast networks in the future, given that the messaging services provided currently and expected for the near future (such as convergent messaging systems) in mobile broadcast networks will continue to more closely approach the functions provided by the Internet.

The problem described above is met currently by each provider or on each platform separately. However, there are no solutions that span across providers or platforms.

DE 102 26 744 B4, which originated with the same applicant, concerns a process and a device to provide a security function in the transmission of data from and to a user terminal device in a mobile communication network. A real-time analysis of the data stream to and from the user terminal device is provided in a device in a network node of the mobile communication network, where data with contents previously defined by the user or a network operator/provider are recognized and processed. As a consequence, the terminal device and any apparatus

of the user linked to it will be protected against attacks from the outside. However, there is the disadvantage that the data must be specified in advance by the user or the network operator/provider to assure optimal protection. But this requires additional costly hardware/software, and in addition, it is possible that critical data (viruses / spam) are not recognized immediately and could thus propagate throughout the receiver's network and networks linked to it.

US 2004/0019651 A1 describes an electronic messaging system with a common filter module to filter out undesired electronic messages. The filter module is installed in the messaging system in common for several receivers and will filter all incoming electronic messages prior to transmittal to the individual receiver.

The invention has an objective of providing a process for convergent messaging systems that will facilitate the exchange of information regarding viruses and spam across network and platform boundaries in order to combat their widespread dissemination.

According to an aspect of the present invention there is provided a method to protect against a virus and/or spam in a mobile broadcast network containing convergent messaging services with transmission of protocol data, the method comprising:

- including a protocol element in the protocol of the convergent messaging services;
- using the protocol element for exchanging virus and/or spam information across network boundaries and platform boundaries, including between network components of at least one network operator,

- wherein, via the distribution protocol, virus and/or spam information is automatically distributed from a sending messaging system by a broker function of the sending messaging system to receiving messaging systems in all network operators linked to the broker function,

- wherein the broker function contains a detailed definition of the receiving messaging systems, and

- wherein the broker function contains information as to which components of the spam/virus information are to be sent to the particular messaging systems of the operators.

In some embodiments, the various network operators (A, B, C ...N) can update the information regarding viruses, such as virus signatures, and/or spam, such as lists of senders etc, in their network elements on a continuous basis.

2a

In some embodiments, the receiving systems can make the decision based on criteria determined by the recipient on whether or not to incorporate the virus and/or spam information in their own virus / spam libraries.

The basic idea of the function provides for the integration of functions in the protocol of a convergent messaging service, which will facilitate the exchange of information on viruses or spam between the network components of a network operator or between several network operators.

Starting from the assumption that the various network operators will continually update information on viruses (such as virus signatures) and spam (sender lists etc.) in their network components, the invention provides for distribution of such information by means of protocol elements of the "convergent message service" to all or a subset of the partner systems (in the own network or in the networks of other operators).

The receiving systems may then decide on the basis of certain criteria, which are defined by the recipient, whether or not to integrate the information into their own virus/spam libraries.

The advantage of such a “linkage” derives from the exchange of information on spam / viruses, which makes it feasible to suppress viruses / spam in the originating network and to preclude their spread to other networks.

Furthermore, the invention also provides that the above information on spam / viruses may also be forwarded automatically by a so-called broker function to all operators linked to the function by way of appropriate protocol elements.

The invention will be described in the following by reference to graphs for a single embodiment. The graphs and their description will reveal other characteristics and advantages of the invention essential to the invention.

The graphs show:

Fig. 1 the transmission of spam / virus data from a first convergent messaging system A to a second convergent messaging system B.

Fig. 2 the transmission of spam / virus data from a first convergent messaging system A to a plurality of convergent messaging systems of operators A, B, C ... N by means of a “broker function.”

Fig. 1 shows the transmission of spam / virus data from a first convergent messaging system of operator A to a second convergent messaging

system of operator B, where the transmission is handled by a protocol element of the convergent messaging service with current spam / virus information.

This spam / virus information may then be added as an update to the spam / virus database of the receiving messaging system of operator B either automatically or filtered on a specific basis.

Fig. 2 shows the transmission of spam / virus data from a first convergent messaging system of operator A to a plurality of convergent messaging systems of operators A, B, C ... to N by means of a "broker function."

The transmission via a protocol element of the convergent messaging service with current spam / virus information is handled by the broker function of the messaging system of operator A, which automatically sends the spam / virus information to the receiving messaging systems of operators B, C, D ... to N. The broker function contains a more detailed definition of the messaging systems of operators B, C, D to N, which receive the spam / virus information, as well as which components of the spam / virus information should be send to the particular messaging system of operators B, C, D to N.

The embodiments of the invention in which an exclusive property or privilege is claimed are defined as follows:

1. A method to protect against a virus and/or spam in a mobile broadcast network containing convergent messaging services with transmission of protocol data, the method comprising:

including a protocol element in the protocol of the convergent messaging services;

using the protocol element for exchanging virus and/or spam information across network boundaries and platform boundaries, including between network components of at least one network operator,

wherein, via the distribution protocol, virus and/or spam information is automatically distributed from a sending messaging system by a broker function of the sending messaging system to receiving messaging systems in all network operators linked to the broker function,

wherein the broker function contains a detailed definition of the receiving messaging systems, and

wherein the broker function contains information as to which components of the spam/virus information are to be sent to the particular messaging systems of the operators.

2. The method of claim 1, wherein the at least one network operator updates the virus and/or spam information in their network components on a continuous basis.

3. The method of claim 2, wherein the virus and/or spam information comprises virus signatures, spam, or lists of senders or any combination thereof.

4. The method of any one of claims 1 to 3, wherein the receiving systems make a decision, wherein the decision is whether or not to incorporate the virus and/or spam information in their own virus and/or spam libraries, and wherein the decision is based on criteria determined by the recipient.

1/1

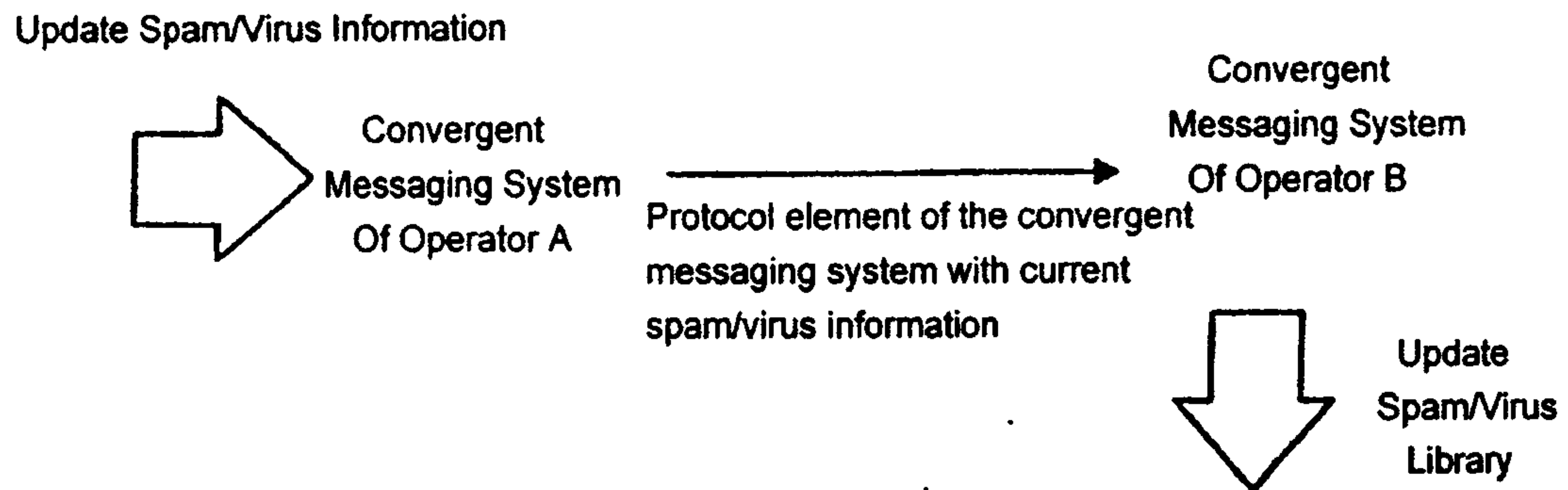


Fig. 1

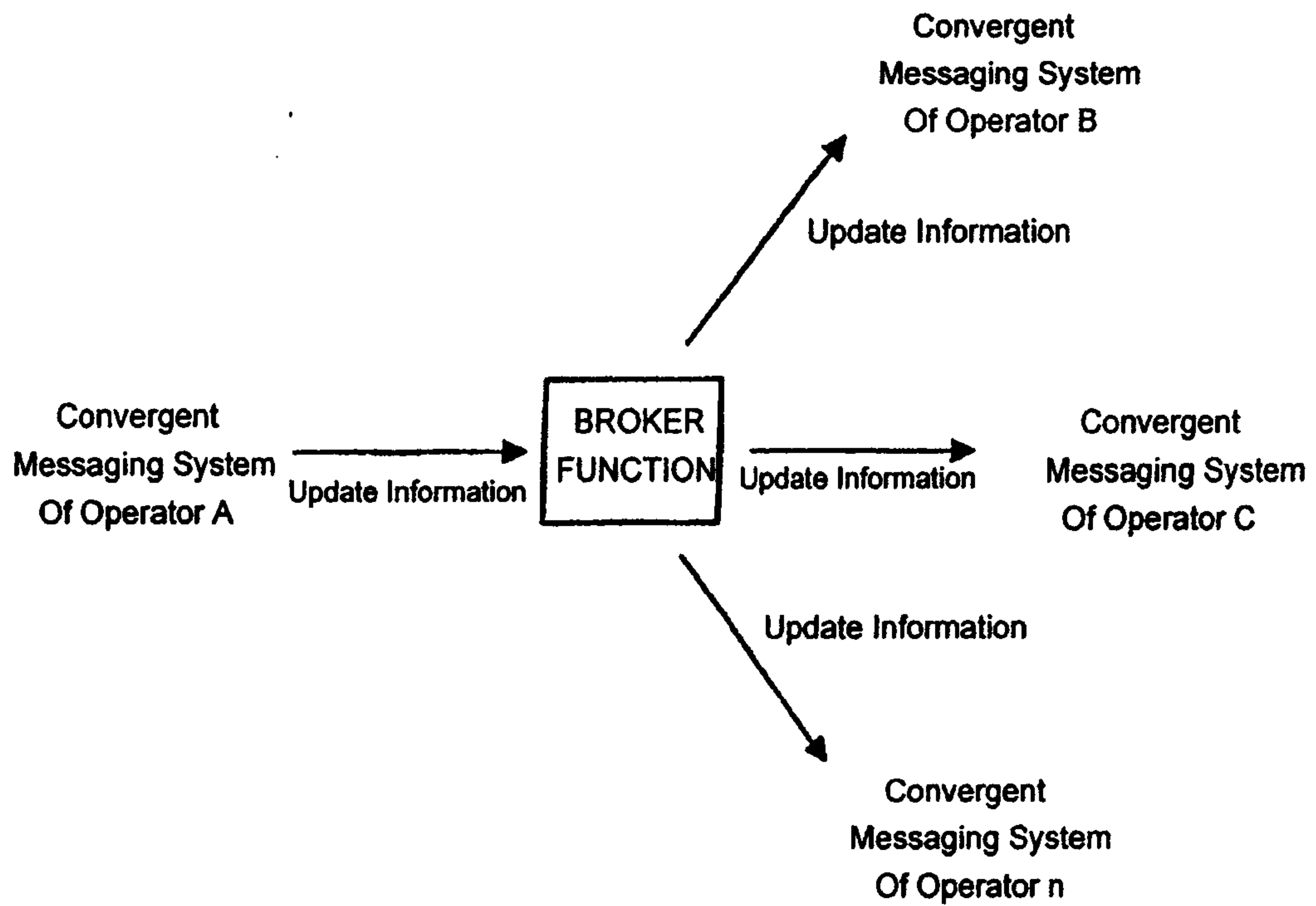


Fig. 2

