DUAL USE COUNTERS FOR ROUTING LOOPS AND SPAM DETECTION

ABSTRACT

A method for detecting an undesirable condition within a messaging network. A message is received and a source of the message is identified. If an entry in a database for the source has not been created, an entry is created. A source counter for the source is then set to one and a timestamp is created for the source. If an entry in the database for the source has been previously created, the source counter is incremented by one and the timestamp is updated. The source counter is then compared to a source threshold, and if the source counter exceeds the source threshold over the course of predetermined amount of time, a source alarm is triggered. A sliding with respect to the predetermined amount of time may also be implemented to account for total counts that may fall across or be split by set periods of time. The invention is particularly useful for detecting “spam” events and undesirable routing loops.

No Figure