(71) Applicants and
(72) Inventors: LAKSHMI NARAYANAN, Ram, Gopal [IN/US]; 2 Kimball Court, Apt. 506, Woburn, MA 01801 (US). LI, Man [CA/US]; 3 Overlook Drive, Bedford, MA 01730 (US).

(74) Agents: ROLNIK, Robert, C. et al.; Nokia Inc., 6000 Connection Drive, Ms 1-4-755, Irving, TX 75039 (US).

(54) Title: CONTEXT FILTER IN A MOBILE NODE
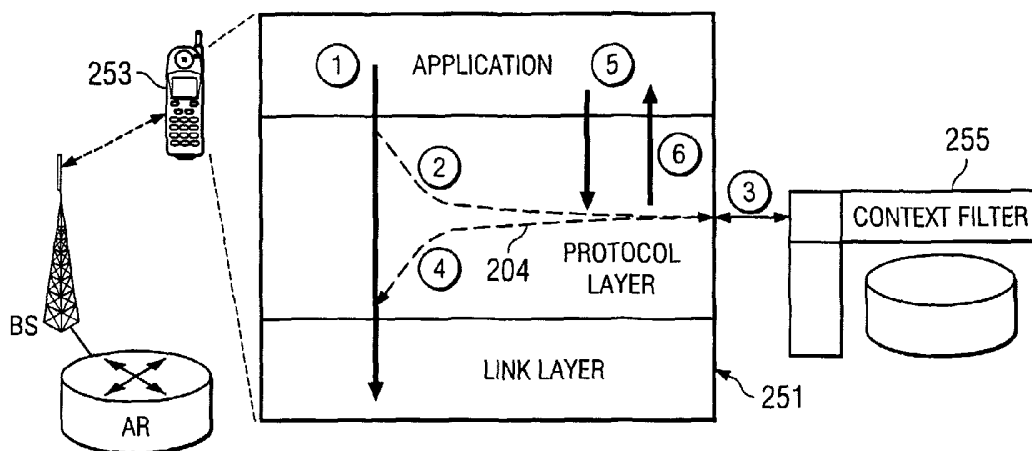
(57) Abstract: In mobile IP networks, a method of forwarding packets of a mobile node. After a mobile node moves from one cell to another which is also know as a handover, the mobile node is informed of the capability changes in the access router and the new communication path. There is also a filter mechanism (255) inside the mobile node to filter out messages that will be rejected by the new access router due to changes resulting from a handover.

CONTEXT FILTER IN A MOBILE NODE

Background

[0001]   In mobile IP networks, when a mobile node (MN) moves from one cell to another, handover occurs. The result of the handover is that the MN connects to the network through a new access router (AR). The handover may occur between access routers of the same or different administrative domains. In all cases, the information related to the mobile node has to be transferred from the old AR to the new AR in order to minimize the effect of the change of access routers. This is the so-called context transfer.

[0002]   During inter handovers, context related to MN are moved from old access router (say AR1) to new access router (say AR2). It may happen that the new access router AR2 or the new communication path established cannot meet the needs of existing active sessions or possible future sessions. For example, it may be that the available bandwidth along the new path is less than that of the previous one. Hence QoS may degrade. It may also be that AR2 does not support an encryption algorithm the MN may request for its future communication sessions. In all these cases, if the MN is not informed about the changes, the services to existing sessions may be degraded or compromised. In addition, the MN may send messages to initiate new sessions and those messages may be rejected by AR2 because AR2 cannot support the required services. This results in a waste of wireless bandwidth.

[0003]   In wireless networks, bandwidth is a precious resource. Every effort should be make to efficiently utilize this resource. The above-mentioned references are exemplary only and are not meant to be limiting in respect to the resources and/or technologies available to those skilled in the art.

Summary

[0004]   The proposals in this invention comprise two aspects. First, we propose a mechanism where after a handover the MN is informed of the capability changes in AR and the new communication path. Second we propose a filter mechanism inside the MN to filter out messages that will be rejected by the new AR due to changes resulted from a handover.

Brief Description of the Drawings

[0005]   The disclosed inventions will be described with reference to the accompanying drawings, which show important sample embodiments of the invention, wherein:

[0006]   Fig. 1 is a reference system for transferring context of a mobile node between autonomous systems; and

[0007]   Fig. 2 shows how and when these filters are applied and used for normal operation.

Detailed Description

[0008]   An embodiment may inform the Mobile Node (MN) about the changes of Access Router (AR) capabilities or the communication path. The MN will perform context filters for both incoming and outgoing packets accordingly. The advantages this embodiment may provide are:

[0009]   1.   Efficient utilization of wireless spectrum, by making decisions on the MN for out going packets;

[0010]   2.   For incoming packets received from the new access routers, the "context filter " rules are applied and, in case the packets get rejected, then these packets may be generated by hacker who is interested in attacking the MN;

[0011]   3.   If the service is degraded, and if there is an application level signaling, this is communicated to the application and the service levels may be renegotiated;

[0012]   4.   Reduces number of filtering rules in the Access routers and improves the performance significantly;

[0013]   5.   Seamless approach to change the subscription profile by the MN; and

[0014]   6.   This approach works as an extension to personal firewall on all MN.

[0015]   Figure 1 shows the reference architecture for the context transfer framework. For example, when the MN 101 that is in AS1 121 moves to AS2 131, as per Policy based mechanisms for selecting access routers and mobile context relocation", submitted IPR, U.S. app. No. 60/336,937, Docket No. NC17419P, the context transfer takes place. It may happen that the new access router, e.g. AR2, 133 or the new communication path established cannot meet the needs of existing active sessions or possible future sessions. For example, it may be that the available bandwidth along the new path is less than that of the previous one. Hence QoS may degrade. It may also be that AR2 133 does not support an encryption algorithm the MN 101 may request for its future communication sessions.

[0016]   An embodiment allows, after the context transfer is complete, AR2 133 sends the MN 101 a context completion message that includes the changes with AR capabilities and communication paths. The MN 101 then updates the working set filter accordingly.

[0017]   Fig. 2 shows how and when these filters are applied and used for normal operation in an exploded view of MN stack.

[0018]   Precondition:

[0019]   For example, MN **253** has started to roam (either in home network or switched on in the different network) in either case the context filter is created. The AR that is currently serving the MN **253** through Base Station (BS) updates the MN servicing profile to the MN **253**. Upon receiving this message, MN **253** creates a context working set filters.

[0020]   Operation (1):

[0021]   1.   For example, Application 251 (say A) has started and wants to communicate to its CN.

[0022]   2.   Protocol stack in the MN **253** consult the context filters **255**

[0023]   3.   Context filters rules are applied based on the current working set

[0024]   4.   If the capabilities are meet then the packet is forwarded to the Core Network (CN)

[0025]   Operation (2):

[0026]   1.   For example, Application (say A) has started and wants to communicate to its CN.

[0027]   2.   Protocol stack in the MN **253** consult the context filters **255**

[0028]   3.   Context filters rules are applied based on the current working set

[0029]   4.   If the context filter rules are not meet then the protocol layer generates an error **204** (may be ICMP error) informing that this application cannot be executed and the application requirements are not meet.

[0030]   5.   It is up to the application to decide what to do next. It may give up or it may, for example, lower its requirements and initiate another session. In either case, messages that would be rejected by Access Router (AR) are never sent into the network.

<u>What is claimed is:</u>

[0031] 1. A method for forwarding a packet of a mobile node, said mobile node in communication with an access router, said mobile node having a current working set and said access router having at least one capability comprising the steps of:

[0032] providing the packet to a protocol stack;

[0033] consulting a context filter;

[0034] applying at least one context filter rule based on the current working set; and

[0035] forwarding the packet based on at least one capability.

[0036] 2. The method for forwarding a packet of claim 1 further comprising the step of:

[0037] creating a context working set filter prior to the step of providing the packet to a protocol stack.

[0038] 3. The method for forwarding a packet of claim 2 further comprising the step of:

[0039] updating a mobile node servicing profile prior to the step of creating a context working set filter.

[0040] 4. A method for forwarding a packet of a mobile node, said mobile node in communication with an access router, said mobile node having a current working set comprising the steps of:

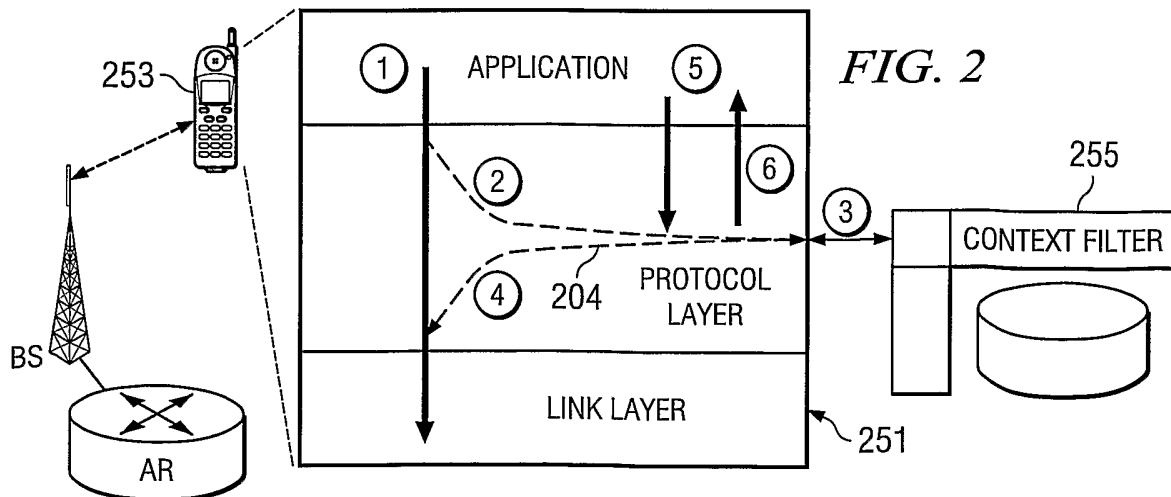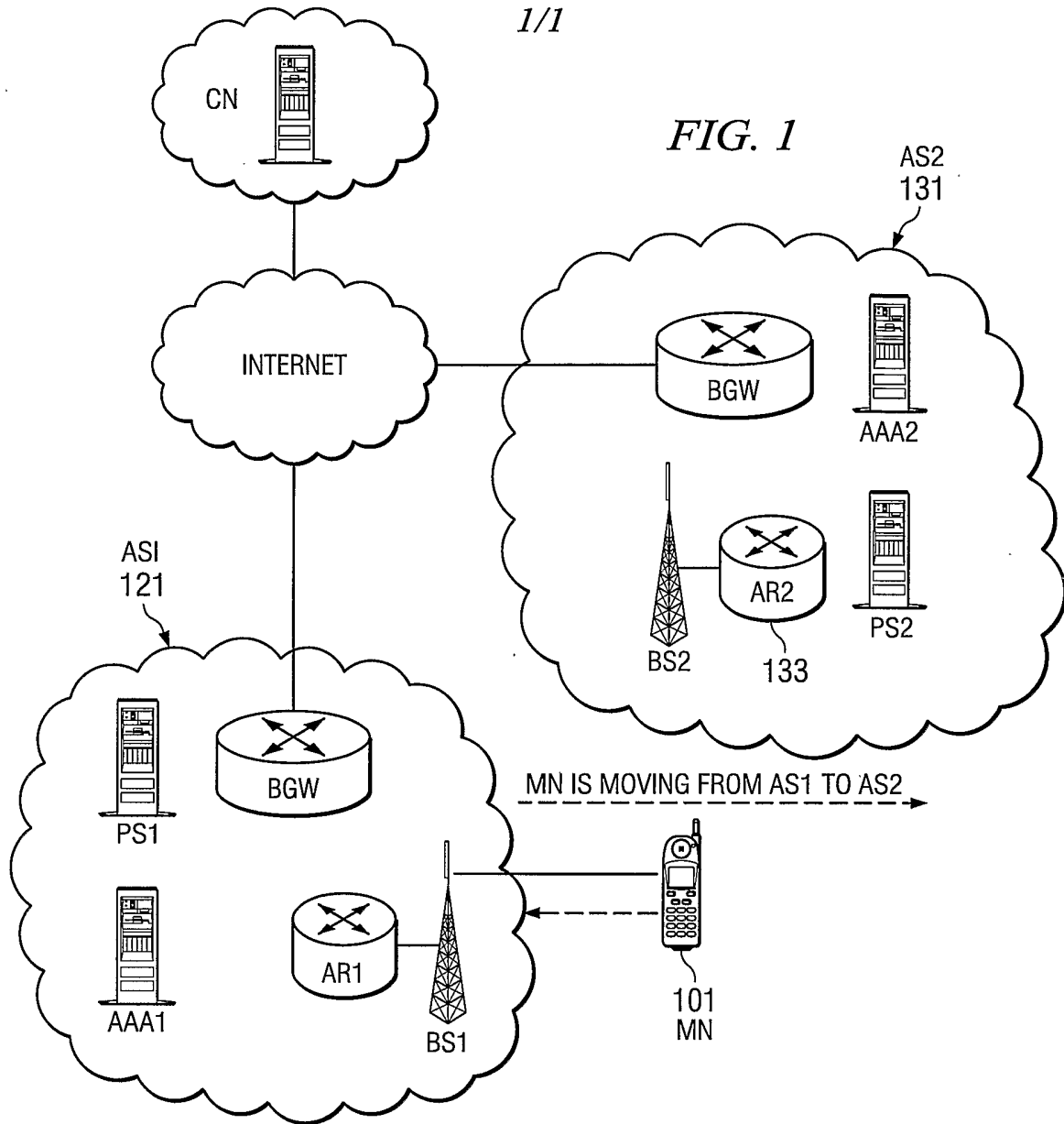**[0041]** starting an application;

[0042] consulting a context filter;

[0043] applying at least one context filter rule based on the current working set; and

[0044] generating an error provided that the at least one context filter rule is not met.

[0045]   5. The method of forwarding of claim 4 further comprising the step of initiating a session.

[0046]   6. The method of forwarding of claim 5 further comprising the step of giving up.

[0047]   7. The method of forwarding of claim 4 wherein the step of generating an error comprises the step of generating an ICMP error.

1/1

FIG. 1

MN IS MOVING FROM AS1 TO AS2

FIG. 2

INTERNATIONAL SEARCH REPORT

A. CLASSIFICATION OF SUBJECT MATTER
IPC(7) : H04Q 7/00; G06F 15/16
US CL : 370/331; 709/227
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)
　　U.S. : 370/331; 709/227

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 practicable, search terms used)
ACM, IEEE

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X, P	GOUDA et al. "Hop Integrity in Computer Networks" IEEE Transactions on Networking, June 2002, Volume 10, No. 3, pages 308-319.	1-7
X	US 2001/0017862 A1 (TOKUYO et al) 30 August 2001 (30.08.2001), the whole document.	1-7
X	SHARMA et al. "Quality of Service Guarantee on 802.11 Networks", HOT Interconnects 9, 22-24 August 2001, pages 99-103.	1-7
A	CACERES et al. "Fast and Scalable Handoffs for Wireless Internetworks", MOBICOM '96, pages 56-66.	1-7
A	US 5 442 633 A (PERKINS et al) 15 August 1995 (15.08.1995), the whole document.	1-7
A, P	YOKOTA et al. "Link Layer Assisted Mobile IP Fast Handoff Method over Wireless LAN Networks", MOBICOM '02, 23-28 September 2002, pages 131-139.	1-7

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:	"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
"A" document defining the general state of the art which is not considered to be of particular relevance	
"E" earlier application or patent published on or after the international filing date	"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
"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)	"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
"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	"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
18 March 2003 (18.03.2003)	02 APR 2003
Name and mailing address of the ISA/US	Authorized officer
Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231	David Wiley
Facsimile No. (703)305-3230	Telephone No. 703-746-7240

Form PCT/ISA/210 (second sheet) (July 1998)