Trials@uspto.gov
571-272-7822

Paper 11
Entered: August 6, 2014

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

ERICSSON INC.,
Petitioner,

v.

INTELLECTUAL VENTURES I LLC,
Patent Owner.

Case IPR2014-00527
Patent 7,496,674 B2

Before JOSIAH C. COCKS, WILLIAM A. CAPP, and DAVID C. McKONE, *Administrative Patent Judges.*

CAPP, *Administrative Patent Judge.*

DECISION
Institution of *Inter Partes* Review
37 C.F.R. § 42.108

Ericsson Inc. ("Ericsson") filed a corrected Petition (Paper 8, "Pet.") requesting *inter partes* review of claims 1–22 of U.S. Patent No. 7,496,674 B2 (Ex. 1001, the "'674 patent"). Intellectual Ventures I LLC ("Intellectual Ventures") filed a Patent Owner Preliminary Response (Paper 10, "Prelim. Resp."). We have jurisdiction under 35 U.S.C. § 314(a). We conclude that Ericsson has shown a reasonable likelihood of prevailing in challenging claims 1–22, and we institute *inter partes* review as to such claims.

I. BACKGROUND

A. The '674 patent (Ex. 1001)

The '674 patent, titled "System, Method, and Base Station Using Different Security Protocols on Wire And Wireless Portions of Network," relates to a method and apparatus for sending and receiving datagrams on wired and wireless portions of a network. Ex. 1001, claims 1, 13. The invention implements security protocols on transmissions over wired and wireless portions of the network. *Id.* A first security protocol is implemented on transmissions over the wired portion of the network. *Id.* A second and different security protocol is implemented over the wireless portion of the network. *Id.*

The invention employs a wireless base station. *Id*. The base station interfaces with both the wired and wireless portions of the network. *Id.* Processing of datagrams to implement the first and second security protocols is performed in the base station. *Id.*

B. Challenged Claims

Ericsson challenges claims 1–22. Claims 1, 13, and 18 are independent claims. Claim 1 is a method claim and claim 13 is an apparatus claim. Claims 1 and 13 (with paragraph indentation added) are reproduced below:

> 1. A method comprising:
>
> receiving a first packet from a wired data network in a wireless base station that is coupled to the wired data network,
>
> wherein the first packet is protected according to a first security protocol on the wired data network, and
>
> wherein a target device of the first packet communicates with a source of the first packet, at least in part, over a wireless network on which the wireless base station communicates;
>
> processing the first packet in the wireless base station according to the first security protocol;
>
> determining that the first packet is targeted at the target device, wherein the determining is performed by the wireless base station, and
>
> wherein the first packet comprises a header coded with address information identifying the target device; and
>
> applying a second security protocol employed on the wireless network to the first packet, wherein the second security protocol is different from the first security protocol, and wherein the applying is performed in the wireless base station.
>
> 13. A base station comprising:
>
> a first interface configured to couple to a wired data network in use;
>
> a second interface configured to transmit and receive on a wireless network in use; and

a controller coupled to the first interface and the second interface, wherein the controller is configured to process a first packet received by the first interface,

wherein the controller is configured to process the first packet according to a first security protocol on the wired data network,

wherein a target device of the first packet communicates with a source of the first packet, at least in part, over the wireless network, and

wherein the first packet comprises a header coded with address information identifying the target device,

wherein the controller is configured to determine that the first packet is targeted at the target device, and

wherein the controller is configured to apply a second security protocol employed on the wireless network to the first packet,

wherein the second security protocol is different from the first security protocol.

C. The Asserted Grounds of Unpatentability

Ericsson challenges claims 1–22 of the '674 patent based on the alleged grounds of unpatentability set forth in the table below, as further supported by the Declaration of Armand M. Makowski, Ph.D. (Ex. 1013).

References	**Basis**	**Claims challenged**
Stadler (Ex. 1003)[1]	§ 102	1-6 and 10-22
Stadler and Davison (Ex. 1010)[2]	§ 103	7-9

[1] J. Scott Stadler and Jay Gelman, *Performance Enhancement for TCP/IP On a Satellite Channel*, MIT Lincoln Laboratory, Lexington, MA © 1998.

[2] U.S. Patent No. 6,829,242 B2 to Davison, *et al*, entitled *Method and Apparatus For Associating PVC Identifiers With Domain Names of Home Gateways*, issued Dec. 2004.

Rai (Ex. 1004)[3]	§ 103	1, 10-13, 17, 18, and 22
Rai and Davison	§ 103	2-9, 14-16, and 19-21
Forslöw (Ex. 1006)[4]	§ 102	1, 10, 13, and 18
Forslöw and Davison	§ 103	2, 4, and 5

D. Claim Interpretation

Claims of unexpired patents are construed by applying the broadest reasonable interpretation, in light of the specification. 37 C.F.R. § 42.100(b).

1. "security protocol"

The term "security protocol" appears in each challenged claim.

Ericsson's proposed construction:

> a protocol which enables at least one of (a) authentication or (b) confidentiality via (b1) encryption and/or (b2) tunneling when routing a packet through a network.

Pet. 17.

Intellectual Ventures's proposed construction:

> a protocol that provides security measures.

Prelim. Resp. 3.

Intellectual Ventures criticizes Ericsson's proposed construction as artificially expanding the definition of "security protocol" to include "tunneling." Prelim. Resp. 5. Intellectual Ventures argues that "tunneling" does not provide "security." Prelim. Resp. 6.

---

[3] U.S. Patent No. 6,414,950 B1 to Rai, *et al*, entitled *Sequence Delivery of Messages*, issued Jul. 2, 2002.

[4] U.S. Patent No. 6,608,832 B2 to Forslöw, entitled *Common Access Between A Mobile Communications Network And An External Network With Selectable Packet-Switched And Circuit-Switched And Circuit-Switched Services*, issued Aug. 19, 2003.

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.