US005809412A

United States Patent [19]

Daurio et al.

[11] **Patent Number: 5,809,412**

[45] **Date of Patent: Sep. 15, 1998**

[54] **SYSTEM FOR DETECTING A FRAUDULENT REMOTE UNIT WHICH UPON DETECTION PLACES A CALL TO THE CELLULAR INFRASTRUCTURE USING IDENTIFICATION IN FORMATION OF THE FRAUDULENT REMOTE UNIT**

[75] Inventors: **Suzanne Daurio**, McHenry; **Michael Duda**, Naperville; **Tom Joyner**, Chicago; **Eric Drury**, Lake Zurich, all of Ill.

[73] Assignee: **Motorola, Inc.**, Schaumburg, Ill.

[21] Appl. No.: **716,590**

[22] Filed: **Sep. 18, 1996**

[51] **Int. Cl.**[6] **H04Q 7/00**; H04Q 9/00

[52] **U.S. Cl.** **455/410**; 455/411

[58] **Field of Search** 455/410, 411, 455/425, 67.1; 380/23, 25; 324/76.12; 379/189

[56] **References Cited**

U.S. PATENT DOCUMENTS

4,955,049	9/1990	Ghisler	379/58
5,005,210	4/1991	Ferrell	455/115
5,329,591	7/1994	Magrill	380/25
5,345,595	9/1994	Johnson et al.	455/33.1
5,420,910	5/1995	Rudokas et al.	379/59
5,555,551	9/1996	Rudokas et al.	379/59

FOREIGN PATENT DOCUMENTS

3441724	5/1986	Germany .

OTHER PUBLICATIONS

"EMX 2500 Features and Enhancements" section #68P09222A54–O, Motorola's Clone Clear™, Technical Education and Documentation, Aug. 14, 1994.

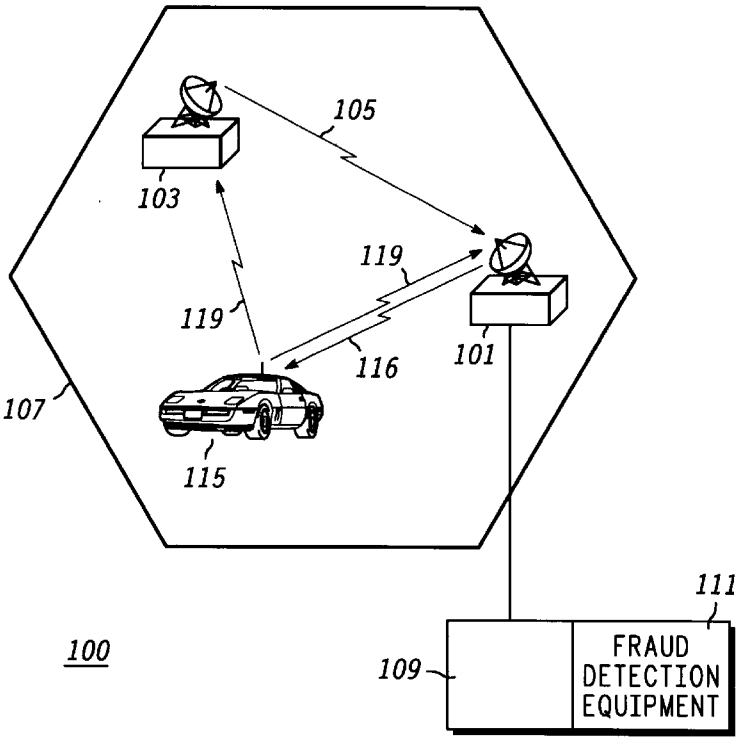
"PhonePrint™, Cellular Fraud Control System Description", Corsair Communications.

Primary Examiner—Tommy P. Chin
Assistant Examiner—David R. Vincent
Attorney, Agent, or Firm—Kenneth A. Haas

[57] **ABSTRACT**

Detection of a fraudulent remote unit **(113)** in a communication system **(100)** occurs by external fraud detection equipment **(103)** located external to, and in proximity to a base site **(101)**. External fraud detection equipment **(103)** communicates with base site **(101)** via an uplink communication signal **(105)** and utilizes fraud detection methods not utilized by internal fraud detection equipment **(111)** to identify the remote unit **(113)** as being fraudulent. Once the remote unit **(113)** is identified by the external fraud detection equipment **(103)** as being fraudulent, the external fraud detection equipment **(103)** places an origination order to the base site **(101)** and supplies identification information on the fraudulent remote unit **(113)**. Infrastructure equipment **(109)** utilizes information supplied to it by the external fraud detection equipment **(103)** and disconnects the fraudulent remote unit **(113)**.

13 Claims, 3 Drawing Sheets



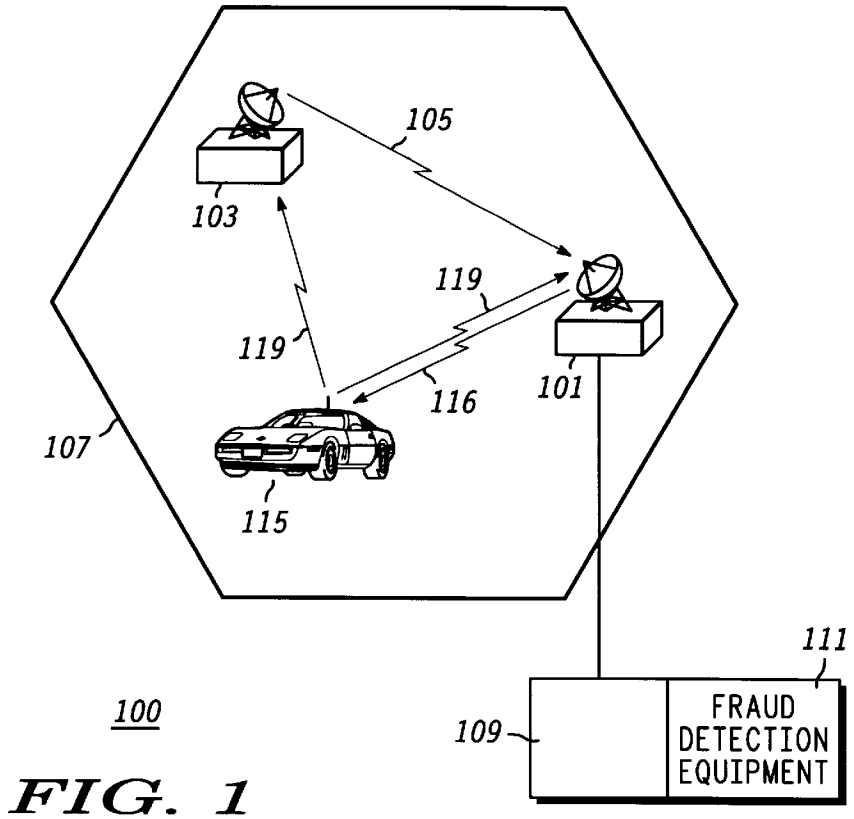
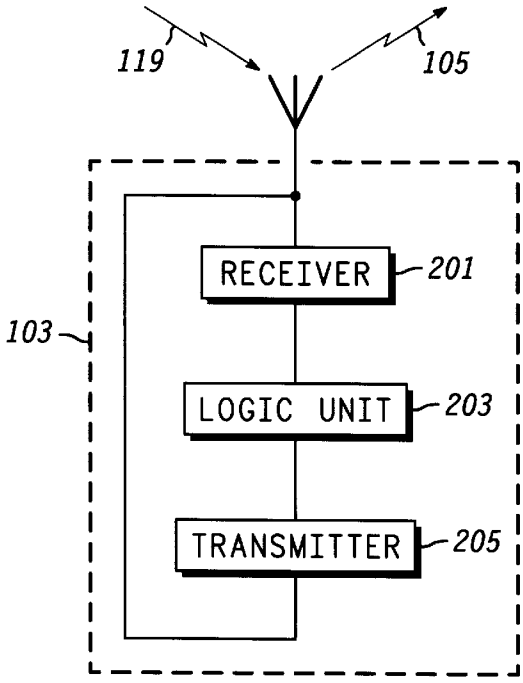


FIG. 1

FIG. 2



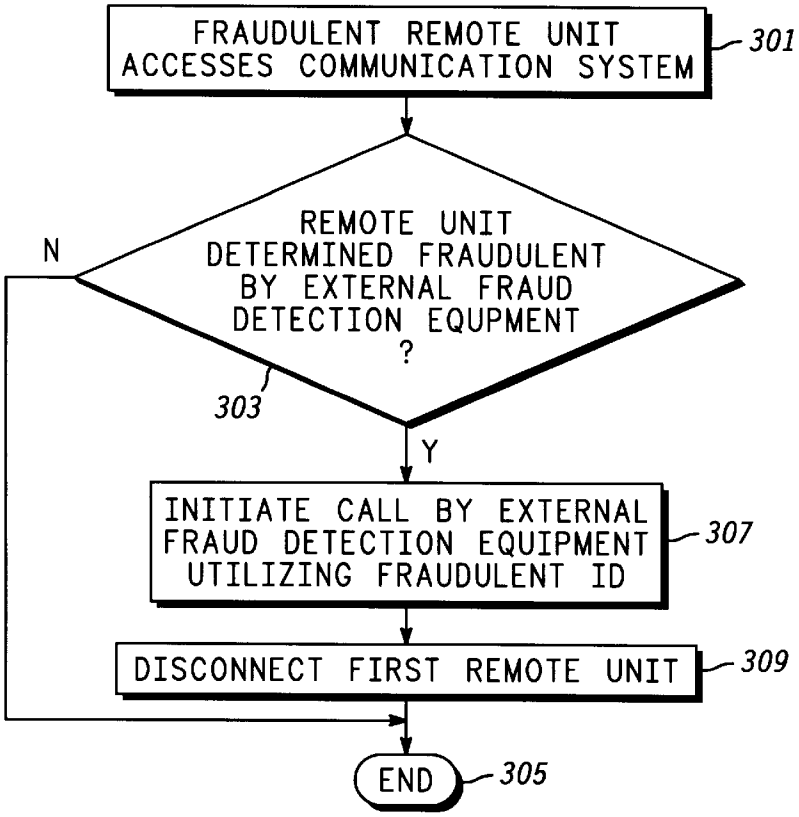
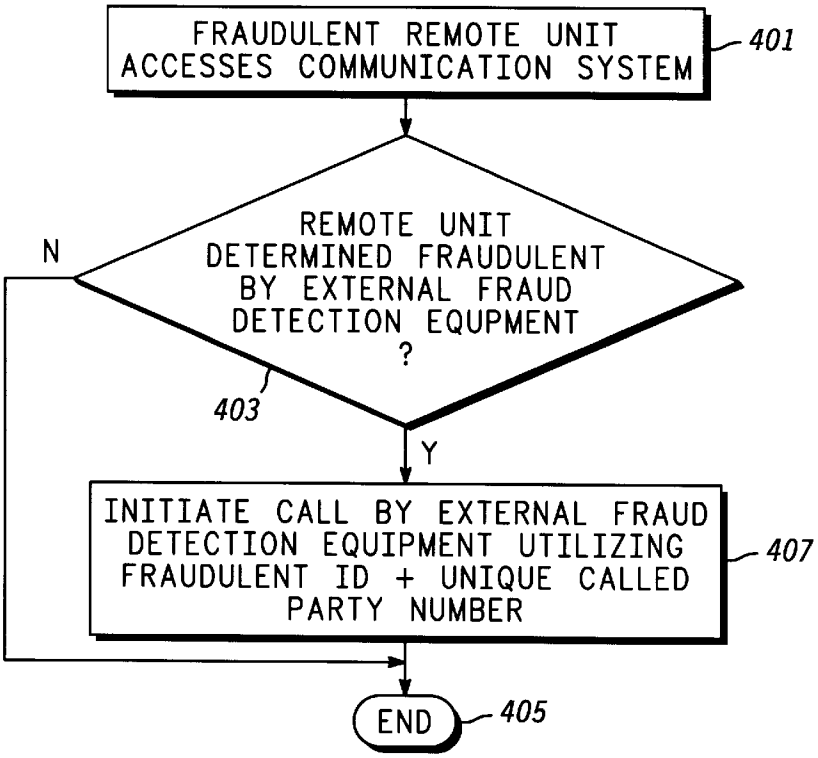


FIG. 3

FIG. 4



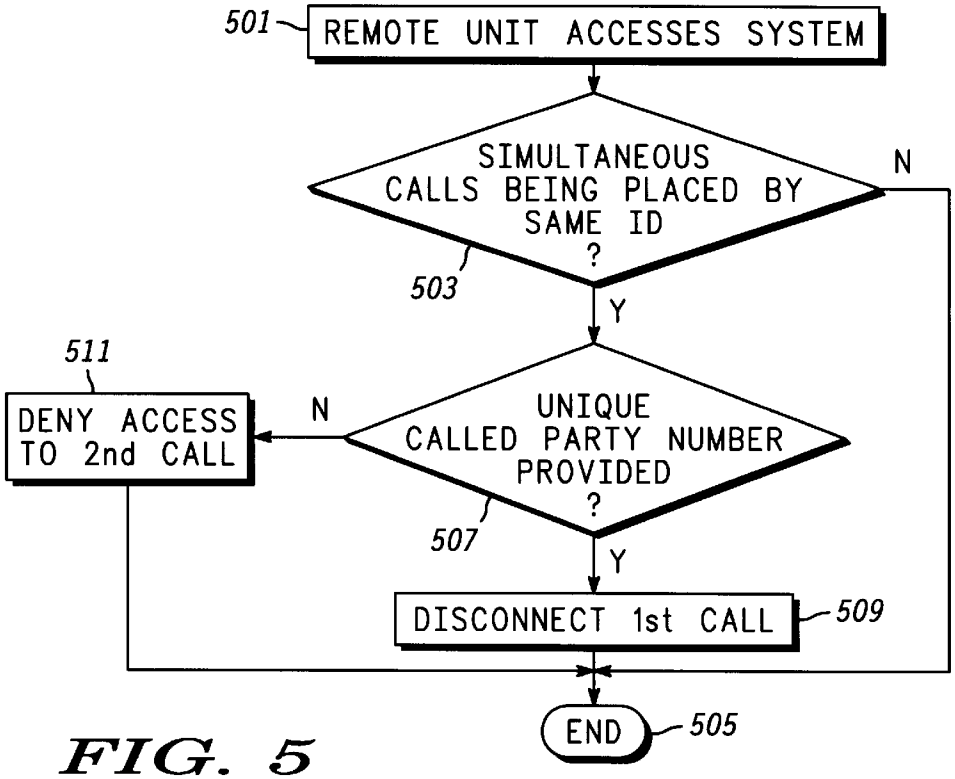


FIG. 5

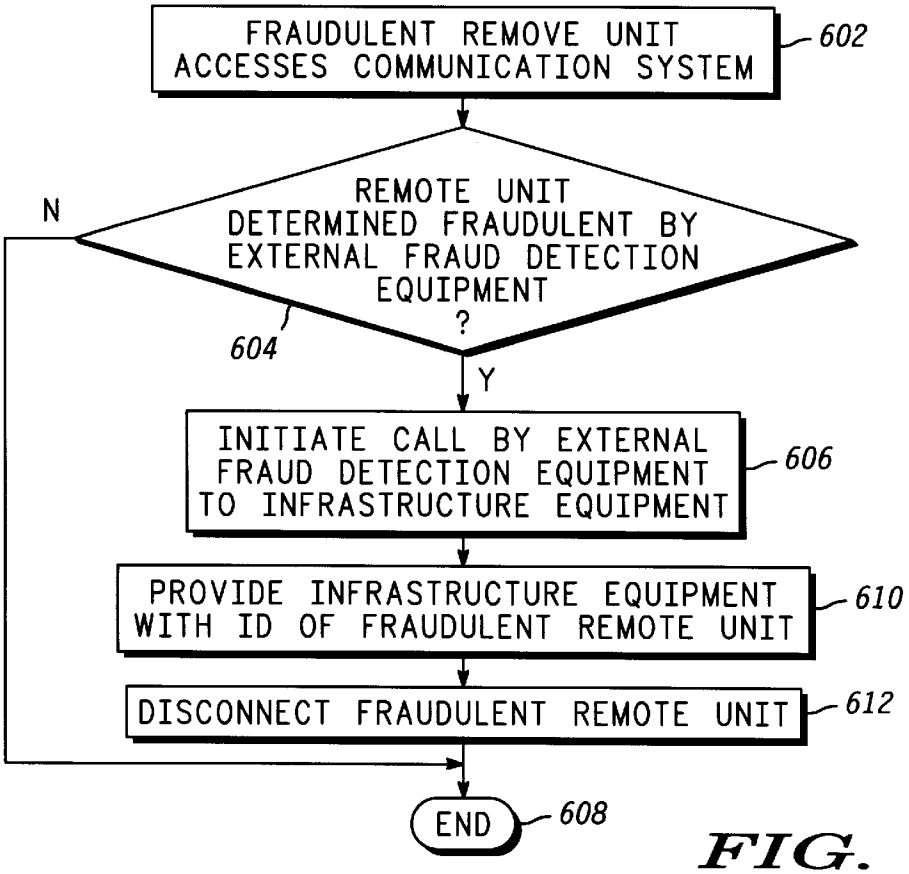


FIG. 6

SYSTEM FOR DETECTING A FRAUDULENT REMOTE UNIT WHICH UPON DETECTION PLACES A CALL TO THE CELLULAR INFRASTRUCTURE USING IDENTIFICATION IN FORMATION OF THE FRAUDULENT REMOTE UNIT

FIELD OF THE INVENTION

The present invention relates generally to cellular communication systems and, in particular, to detection of fraudulent users in cellular communication systems.

BACKGROUND OF THE INVENTION

Communication systems are known to comprise a plurality of base sites that provide communication services to remote units located in corresponding service coverage areas of the base sites. A remote unit (e.g., a mobile or stationary remote unit) that desires to communicate, sends a channel request signal and identification information to a base site serving the coverage area in which the remote unit resides. Identification information includes, but is not limited to, a mobile identification number (MIN) and an electronic serial number (ESN). Upon receiving the remote unit's identification information and channel request signal, the serving base site allocates a communication resource for the remote unit. The communication resource comprises a coordinated pair of frequencies (i.e., an uplink frequency and a downlink frequency sometimes referred to as voice or traffic channels). In a communication system employing a Time Division Multiple Access (TDMA) protocol, the communication resource comprises a coordinated pair of time slots and frequencies (i.e., a first time slot at an uplink frequency and a second time slot at a downlink frequency). The uplink frequency supports transmissions from the remote unit to the serving base site, whereas the downlink frequency supports transmissions from the serving base site to the remote unit.

Upon allocating the communication resource, the base site sends a channel designation signal containing the uplink and downlink frequency, to the remote unit via a control channel, and upon receiving the channel designation signal, the remote unit tunes its transmitter and receiver to the designated frequencies and begins communicating with a telephone network subscriber or another remote unit via the serving base site. The serving base site then tracks billing information with respect to the call, and utilizing the remote unit's identification information, charges the appropriate fees to the corresponding caller.

There are many ways in which users can place fraudulent calls, resulting in fees associated with the call being charged to individuals who did not place the call. For example, as described in U.S. application Ser. No. 08/651,230 "Method and Apparatus for Detection of Fraudulent Users in a Communication System Using Signaling-Channel Phase Shift" by W. Willey, a fraudulent remote unit (i.e., a fraudulent user operating a remote unit) may hijack a channel by transmitting on a corresponding uplink frequency at a high enough power level, causing the legitimate remote unit to be abandoned in favor of the fraudulent remote unit. Once communication has been established between the fraudulent remote unit and the communication system, the fraudulent remote unit may then utilize three-party calling features of the communication system to place other calls utilizing the legitimate remote unit's identification information, causing associated fees to be charged to the legitimate remote unit.

Another way in which users can place fraudulent calls is by cellular cloning. Cellular cloning involves procuring a remote unit's identification information and reprogramming a fraudulent remote unit with the obtained identification information. The reprogrammed, or cloned remote unit simply places a call using the identification information of the legitimate remote unit, causing associated fees to be charged to the legitimate remote unit.

There exists many methods in which communication systems can detect the placement of fraudulent calls. Typically each fraud detection method requires specific software and hardware existing within the system's infrastructure equipment, and can be very costly to implement. This can prevent system operators from outfitting existing infrastructure equipment with new fraud detection equipment. Thus a need exists for a method and apparatus for detection of fraudulent users in a communication system that is less costly and does not require outfitting existing infrastructure equipment with additional fraud detection equipment when new fraud detection methods are devised.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. **1** illustrates a communication system in accordance with the preferred embodiment of the present invention.

FIG. **2** is a block diagram of the external fraud detection equipment of FIG. **1** in accordance with the preferred embodiment of the present invention.

FIG. **3** is a flow chart illustrating operation of the external fraud detection equipment of FIG. **1** in accordance with a preferred embodiment of the present invention.

FIG. **4** is a flow chart illustrating operation of the internal fraud detection equipment of FIG. **1** in accordance with an alternate embodiment of the present invention.

FIG. **5** is a flow chart illustrating operation of the external and internal fraud detection equipment of FIG. **1** in accordance with a second alternate embodiment of the present invention.

FIG. **6** is a flow chart illustrating operation of the external and internal fraud detection equipment of FIG. **1** in accordance with a second alternate embodiment of the present invention.

DETAILED DESCRIPTION OF THE DRAWINGS

Stated generally, detection of a fraudulent remote unit in a communication system occurs by external fraud detection equipment located external to, and in proximity to a base site. The external fraud detection equipment communicates with the base site via an uplink communication signal and utilizes fraud detection methods not utilized by internal fraud detection equipment to identify the remote unit as being fraudulent. Once the remote unit is identified by the external fraud detection equipment as being fraudulent, the external fraud detection equipment places an origination order to the base site and supplies identification information on the fraudulent remote unit. The infrastructure equipment utilizes information supplied to it by the external fraud detection equipment and disconnects the fraudulent remote unit.

The present invention encompasses a method of detecting a fraudulent remote unit in a communication system by receiving at a point external to cellular infrastructure equipment, a first uplink communication signal transmitted by a remote unit and determining at the point external to the cellular infrastructure equipment, if the first uplink communication signal is transmitted by the fraudulent remote unit. Next, information regarding the fraudulent remote unit is transmitted from the point external to the cellular infrastructure equipment to the cellular infrastructure equipment.

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.