Office de la Propriété Intellectuelle du Canada
Un organisme d'Industrie Canada

Canadian Intellectual Property Office
An agency of Industry Canada

CA 2529654 A1 2005/02/03

(21) 2 529 654

(12) DEMANDE DE BREVET CANADIEN
CANADIAN PATENT APPLICATION

(13) A1

(86) Date de dépôt PCT/PCT Filing Date: 2004/07/02
(87) Date publication PCT/PCT Publication Date: 2005/02/03
(85) Entrée phase nationale/National Entry: 2005/12/14
(86) N° demande PCT/PCT Application No.: US 2004/021268
(87) N° publication PCT/PCT Publication No.: 2005/010562
(30) Priorité/Priority: 2003/07/18 (60/488,374) US

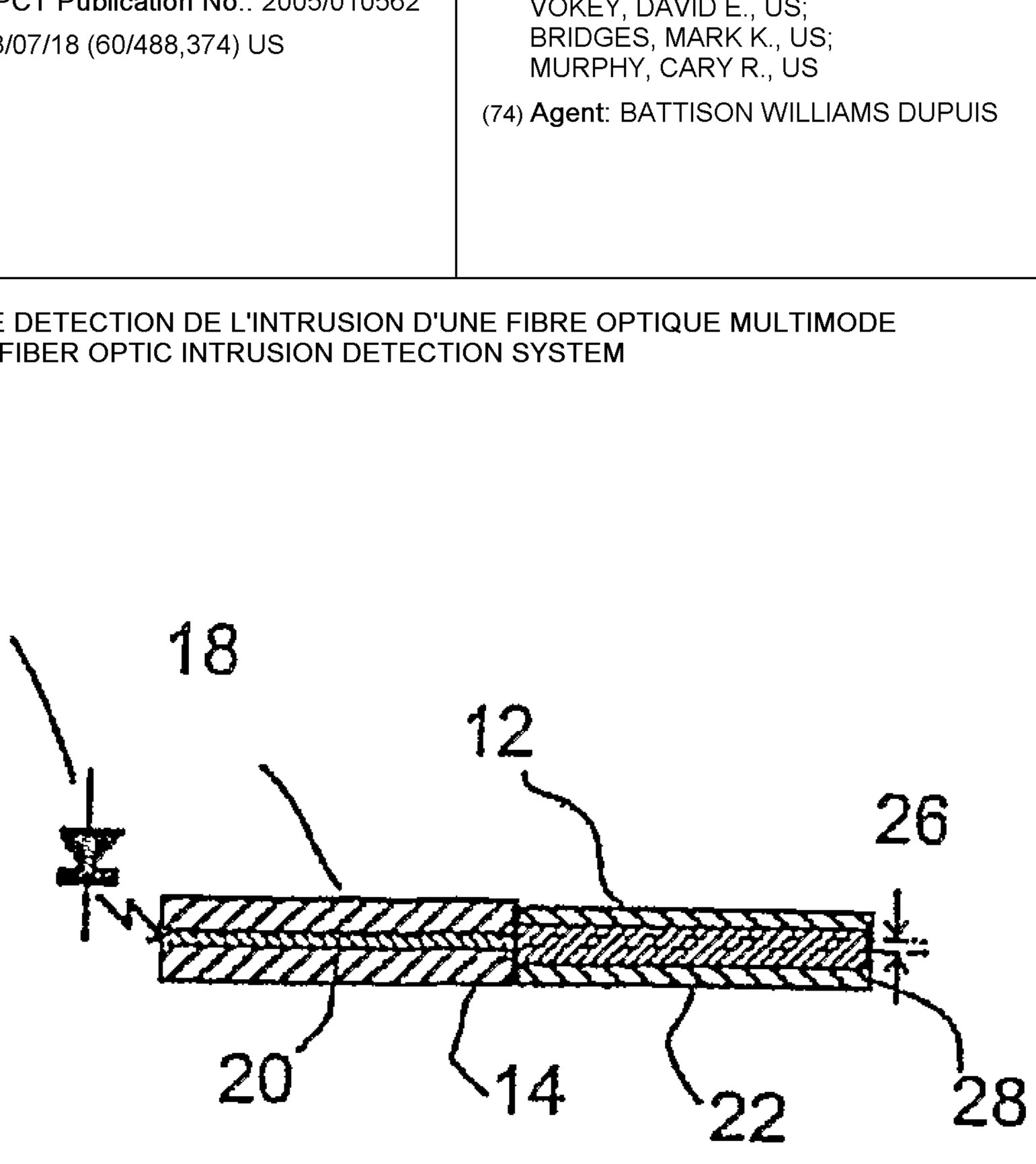
(51) Cl.Int./Int.Cl. *G02B 6/00* (2006.01),
G08B 13/187 (2006.01), *G08B 13/186* (2006.01)

(71) Demandeur/Applicant:
NETWORK INTEGRITY SYSTEMS INC., US

(72) Inventeurs/Inventors:
VOKEY, DAVID E., US;
BRIDGES, MARK K., US;
MURPHY, CARY R., US

(74) Agent: BATTISON WILLIAMS DUPUIS

(54) Titre : SYSTEME DE DETECTION DE L'INTRUSION D'UNE FIBRE OPTIQUE MULTIMODE
(54) Title: MULTIMODE FIBER OPTIC INTRUSION DETECTION SYSTEM



(57) Abrégé/Abstract:
A method and system of intrusion detection for a multimode fiber optic cable (12). A signal is launched into the cable (12) to establish a narrow spectral width, under-filled non-uniform mode field power distribution in the cable (12). A small portion of the higher order signal modes arriving at the remote end (28) of the cable (12) is sampled and monitored for transient changes in the mode field power distribution, which changes with physical disturbance of the cable (12). When changes characteristic of fiber intrusion are detected, an alarm activates. Attempt to access optical fibers in a communication cable can be sensed and alarmed. The active signal of a multimode optical fiber (12) is monitored for signal degradation and transient power disturbance patterns that could indicate fiber damage or physical intrusion. Using adaptive filtering, normal background disturbances from heating/cooling systems, motors, fans and other building systems can be filtered out.

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
3 February 2005 (03.02.2005)

PCT

(10) International Publication Number
WO 2005/010562 A3

(51) International Patent Classification[7]: G02B 06/00, G08B 13/186, 13/187

(21) International Application Number: PCT/US2004/021268

(22) International Filing Date: 2 July 2004 (02.07.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/488,374 18 July 2003 (18.07.2003) US

(71) Applicant *(for all designated States except US)*: **NETWORK INTEGRITY SYSTEMS, INC.** [US/US]; 301 10th Street, N.W., Conover, NC 28613 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **VOKEY, David, E.** [CA/US]; 1206 Northwind Circle, Bellingham, WA 98226 (US). **BRIDGES, Mark, K.** [US/US]; 5475 Chestnut Drive, Hickory, NC 28602 (US). **MURPHY, Cary, R.** [US/US]; 2446 Ashford Drive, Newton, NC 28658 (US).

(74) Agents: **HUNT, Ross, F., Jr.** et al.; Stites & Harbison PLLC, Suite 900, 1199 North Fairfax Street, Alexandria, VA 22314 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

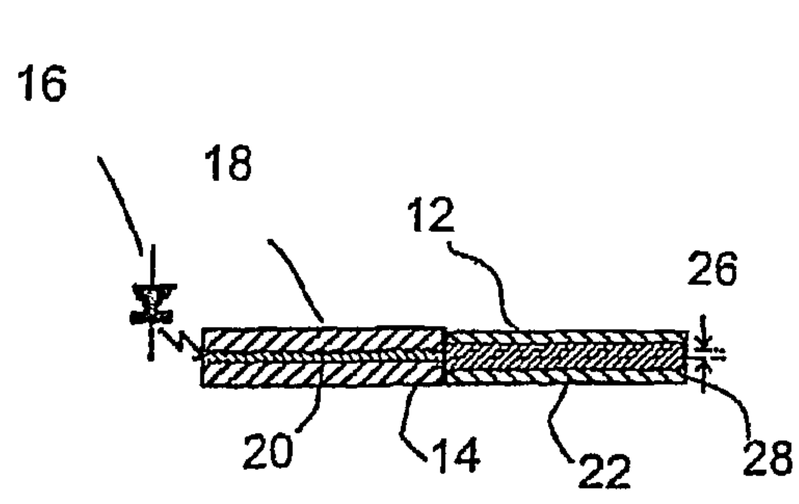
(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

(88) Date of publication of the international search report:
28 July 2005

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: MULTIMODE FIBER OPTIC INTRUSION DETECTION SYSTEM



(57) Abstract: A method and system of intrusion detection for a multimode fiber optic cable (12). A signal is launched into the cable (12) to establish a narrow spectral width, under-filled non-uniform mode field power distribution in the cable (12). A small portion of the higher order signal modes arriving at the remote end (28) of the cable (12) is sampled and monitored for transient changes in the mode field power distribution, which changes with physical disturbance of the cable (12). When changes characteristic of fiber intrusion are detected, an alarm activates. Attempt to access optical fibers in a communication cable can be sensed and alarmed. The active signal of a multimode optical fiber (12) is monitored for signal degradation and transient power disturbance patterns that could indicate fiber damage or physical intrusion. Using adaptive filtering, normal background disturbances from heating/cooling systems, motors, fans and other building systems can be filtered out.

WO 2005/010562 A3

MULTIMODE FIBER OPTIC INTRUSION DETECTION SYSTEM

FIELD OF THE INVENTION

The present invention relates to the detection of physical intrusion into a multimode fiber optic cable.

BACKGROUND

Gigabit Ethernet multimode fiber optic backbone cables are being deployed to connect sections of high-speed networks together. To secure these high-speed networks, software based Intrusion Detection Systems (IDSs) have been introduced. These systems capture and analyze all packets for unusual patterns that point to an intrusion. However, this adds to the complexity of the network. Current IDSs are hampered by a Base-Rate Fallacy limitation, which is the inability to suppress false alarms. Additionally, software-based IDSs do not protect against passive optical fiber tapping, which can go undetected by the network hardware.

It is well known, by those skilled in the technology, that an optical fiber can are easily be tapped and the data stream intercepted. One relatively simple non-interruptive tapping method involves placing a bend coupler on the fiber to be tapped. A controlled bend of a critical radius is placed on the fiber. This causes a small spatial distortion in the core/cladding guiding properties and a fraction of the light escapes the fiber. A detector is located at the point of the light leakage and the data steam intercepted. Bend couplers typically introduce a loss of light power of up to 1 dB or more. Power measuring intrusion detection systems are available to detect this loss in optical power and provide warning alarms.

With care and skill, more insidious methods are available to the skilled intruder. With a sufficiently sensitive receiver and care in preparation, a fiber can be successfully tapped without introducing a telltale bend in the optical fiber. A successful tap can be achieved by carefully removing a short length, in the order of a few centimeters or inches of the protective outer coating of the target fiber and polishing the outer cladding down by a few microns to form a flat coupling region. A cladding-to-

cladding coupling is then made using a special intercept fiber. This method intercepts a portion of the weak but measurable cladding mode power that propagates in the tapped fiber. In this case, the intercepted light, which may be detected by a sensitive receiver, can easily be 20 or 30 dB down from the power in the fiber core. This results in a loss of received optical power of only .04 or .004 dBm and is impossible to detect reliably by power measurement methods. The present invention addresses the limitations of current power loss detection methods and can detect intrusion activity before any optical power loss occurs.

SUMMARY

According to one aspect of the present invention, there is provided a method of detecting intrusion into a multimode fiber optic cable, said method comprising:

launching a light signal into a proximal end of the cable so as to establish a non-uniform mode field power distribution in the cable;

capturing a portion of higher order signal modes arriving at a distal end of the cable;

monitoring the captured portion for transient changes in the mode field power distribution; and

activating an alarm in response to detection of changes in the mode field power distribution that are characteristic of cable handling.

This method can sense and alarm any attempt to access the optical fibers in a fiber optic communication cable. The preferred embodiments of the method monitor the active signal of a multimode optical fiber strand for both signal degradation and transient power disturbance patterns that could indicate fiber damage or physical intrusion.

According to another aspect of the present invention, there is provided a system for detecting intrusion into a multimode fiber optic cable, said system comprising:

a transmitter for launching a light signal into a proximal end of the cable in such a away as to establish a non-uniform mode field power distribution in the cable;

an optic coupler at a distal end of the cable for capturing a portion of higher order signal modes arriving at the distal end of the cable; and

a processor for monitoring the captured portion of the signal to detect transient changes in the mode field power distribution and for activating an alarm in response to detection of changes in the mode field power distribution characteristic of cable handling.

The currently preferred system uses the light output signal from a laser transmitter that is coupled to the multimode fiber in an offset launch alignment. At the distal, receive end of the link, a small percentage of the optical signal is sampled using a specially constructed optic coupler which captures a potion of the higher order mode power. An optical receiver detects the sampled signal and the modal power distribution is monitored for changes. Mechanical disturbances such as handling of the fiber cable cause shifts in the mode power distribution that are detected by the system, which signals a possible intrusion attempt before an actual tap occurs.

Using adaptive filtering, normal background disturbances from heating/cooling systems, motors, fans and other building systems can be learned and filtered out. This will allow maximum sensitivity to intrusion attempt signatures while minimizing the probability of false alarm events. The design objective is to identify intrusion attempts while the attack is still at the outer layer of the cable structure. This will allow for rapid location and interception of any intruder.

BRIEF DESCRIPTION OF THE DRAWINGS

In the accompanying drawings, which illustrate exemplary embodiments of the present invention:

Figure 1 is a longitudinal cross section along line I–I of Figure 2 showing a transmitter for use in a system according to the present invention;

Figure 2 is a transverse cross section of the transmitter, taken along line

I–II of Figure 1;

Figure 3 is a block diagram of the receiver portion of an intrusion detection system according to the present invention; and

Figure 4 is a block diagram of an alternative receiver portion of a system according to the present invention.

DETAILED DESCRIPTION

Referring to the accompanying drawings, and particularly to Figures 1 and 2, a transmitter 10 is illustrated for setting up a narrow spectral width, under-filled, non-uniform mode field power distribution in a multimode optical fiber 12. With this type of mode field, the power distribution in the higher order modes changes with physical disturbance of the fiber, despite the absence of any power loss caused by the disturbance.

The non-uniform high order mode field may be set up in the multimode fiber 12 by illuminating the proximal (near) or transmit end 14 of the fiber with a point source of light that is offset from the centre of the optical fiber core. This can be accomplished by a using a solid-state laser, optical lenses and positioning mechanics. In the illustrated embodiment, however, this is accomplished more simply by launching a solid-state laser 16 into a short length of single mode fiber 18 spliced to the multimode fiber with the centre of its core 20 offset from the centre of the core 22 of the multimode fiber 12 by a fixed offset 26. For typical multimode fibers with either a 50 or 62.5 micron core, the single mode fiber, with a core size of approximately 10 microns, is spliced to the multimode fiber with a micron centre–to-centre offset which is optimized for maximum sensitivity (typically 5 to 20 micron offset).

Referring more particularly to Figure 3, at its distal (remote) or receive end 28 (Figure 1) the multimode optical fiber 12 is connected to a connector 30, the receive port RX_{30} of which delivers the incoming signal from the fiber to the input 32 of a high order mode coupler 34. The coupler taps off a small portion of the higher order modes and returns the remaining optical power to an output port 36. Handling of the fiber cable

will cause a local mechanical disturbance to the fiber. This mechanical disturbance, while not introducing detectable macro or micro bending losses, causes the power distribution in the mode pattern to change. This in turn results in a change of the coupling efficiency of the high order mode coupler and a variation in the optical power at a coupler output 38. The resultant optical signal is proportional in amplitude to the disturbing forces.

The high order mode coupler 34 can be made by a cladding -to-cladding fusion while measuring the tap-coupling ratio during the fusing process using an offset launch source as described.

The main portion of the optical signal is brought from coupler output 36 to the transmit port TX_{40} of an optical connector 40 and is available for a communication or data receiver when active fiber monitoring is employed. The sampled output 38 of the mode coupler is forwarded to a detector and conversion circuit 42 where the optical signal is detected by a photo diode and the resulting electrical output converted from an analog to a digital signal. The digital signal is forwarded to a microprocessor control and communications assembly 44 where the signal is filtered to eliminate normal environmental background noise. The filtered signal is then analyzed for transient signatures and level changes that are characteristic of cable and fiber handling. At a pre-set disturbance level the assembly activates an alarm response. An alarm LED 46 is illuminated on a system status panel 48 and an alarm signal is output to an interface connector 50 for remote alarm reporting.

In the case of active fiber monitoring, where live traffic is carried on the monitored fiber, the laser source 16 can be modulated by a data stream and the output at the far end of the optical path coupled to a data receiver via the output connector 40.

An enhanced variation of the detection scheme is shown in Figure 4. The incoming optical signal is delivered, through connector 30 to the input 32 of the high order mode coupler 34 where the high order mode power distribution is sampled. The output 36 of the high order mode coupler 34 is then transmitted to the input port 52 of a

bulk optics coupler 54. The bulk optics coupler is insensitive to modal power distribution and is used to sample a portion of the total optical signal. The sampled output of the bulk optics connecter 54 is delivered from output port 56 to a second detector circuit 58 where the absolute throughput power is calculated from the fixed ratio sample. This establishes an absolute power baseline that is compared to the high order mode sampling in the microprocessor and communications module 44. The microprocessor then compares the response in the two channels and is able to calculate any power change as well as changes in modal power distribution. Excessive power change levels produce an alarm indication at LED 60, and an alarm signal is sent to connector 50 This provides more information on fiber disturbances as a significant change in both channels could indicate a problem with the laser or fiber path while a transient and steady state change in the high order mode power distribution only would provide a strong indication of an intrusion attempt.

While specific embodiments of the invention have been described in the foregoing, these are presented by way of example only. other embodiments are possible within the spirit and scope of the present invention. In particular, it is to be understood that elements of the system such as the detector and conversion circuit and the microprocessor and communications module may be replaced with any other element or elements for performing similar functions in the system. The invention is to be considered limited solely by the scope of the appended claims

EMBODIMENTS OF THE INVENTION IN WHICH AN EXCLUSIVE PROPERTY OR PRIVILEGE IS CLAIMED ARE DEFINED AS FOLLOWS:

1. A method of detecting intrusion into a multimode fiber optic cable, said method comprising:

launching a light signal into a proximal end of the cable so as to establish a non-uniform mode field power distribution in the cable;

capturing a portion of higher order signal modes arriving at a distal end of the cable;

monitoring the captured portion for transient changes in the mode field power distribution; and

activating an alarm in response to detection of changes in the mode field power distribution that are characteristic of cable handling.

2. A method according to Claim 1 comprising monitoring a fiber strand of the cable for fiber damage or physical intrusion by monitoring an active signal of the strand for both signal degradation and transient power disturbance patterns characteristic of fiber damage or physical intrusion.

3. A method according to Claim 1 further comprising monitoring the mode field power distribution to determine normal background disturbances , and filtering out those normal background disturbances before the detection of changes in the mode field power distribution characteristic of cable handling;

4. A system for detecting intrusion of a multimode fiber optic cable, said system comprising:

a transmitter for launching a light signal into a proximal end of the cable in such a away as to establish a non-uniform mode field power distribution in the cable;

an optic coupler at a distal end of the cable for capturing a portion of higher order signal modes arriving at the distal end of the cable;

a processor for monitoring the captured portion of the signal to detect transient changes in the mode field power distribution and for activating an alarm in response to detection of changes in the mode field power distribution characteristic of

cable handling.

5. A system according to Claim 4 wherein the transmitter comprises a laser transmitter and means for coupling the laser transmitter to the multimode fiber in an offset launch alignment.

6. A system according to Claim 4 wherein the processor includes an adaptive filter comprising a learning module for monitoring the mode field power distribution to determine normal background disturbances therein, and a filter for filtering out those normal background disturbances before analyzing the mode field power distribution for changes characteristic of cable handling.

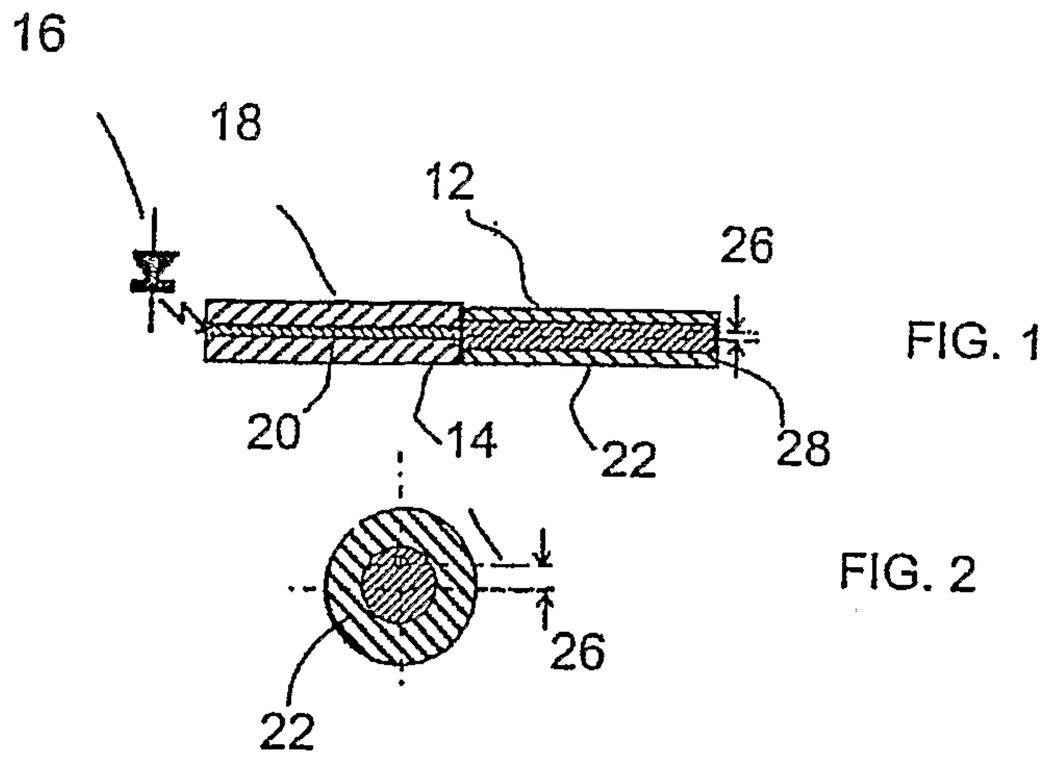


FIG. 1

FIG. 2

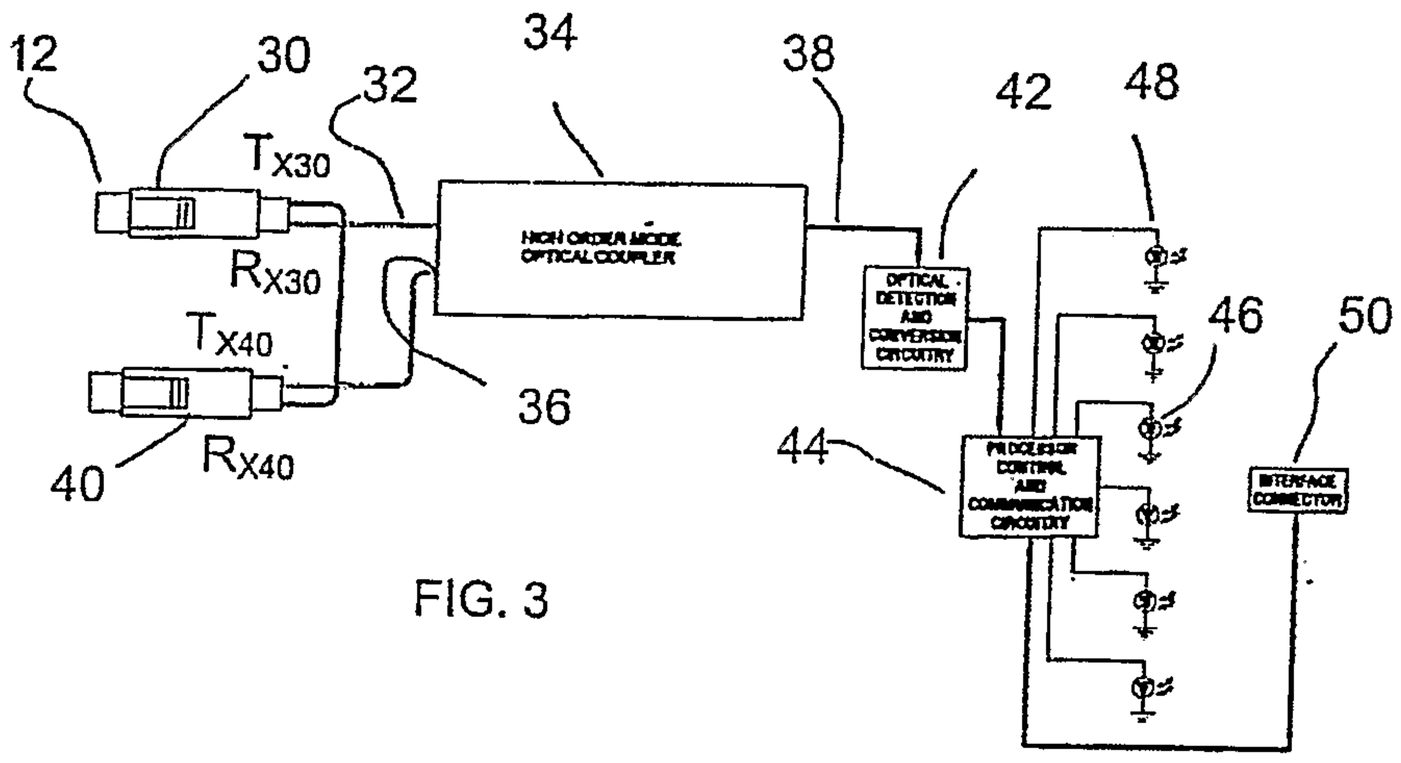


FIG. 3

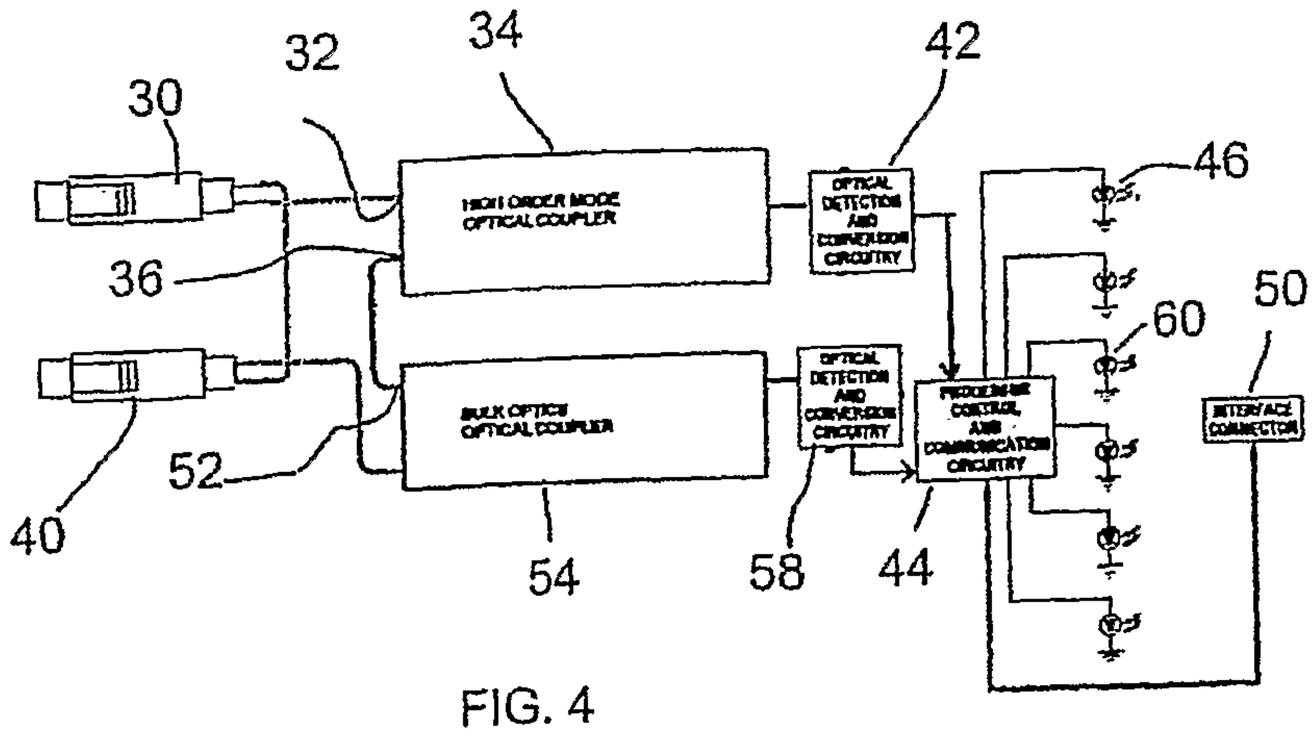
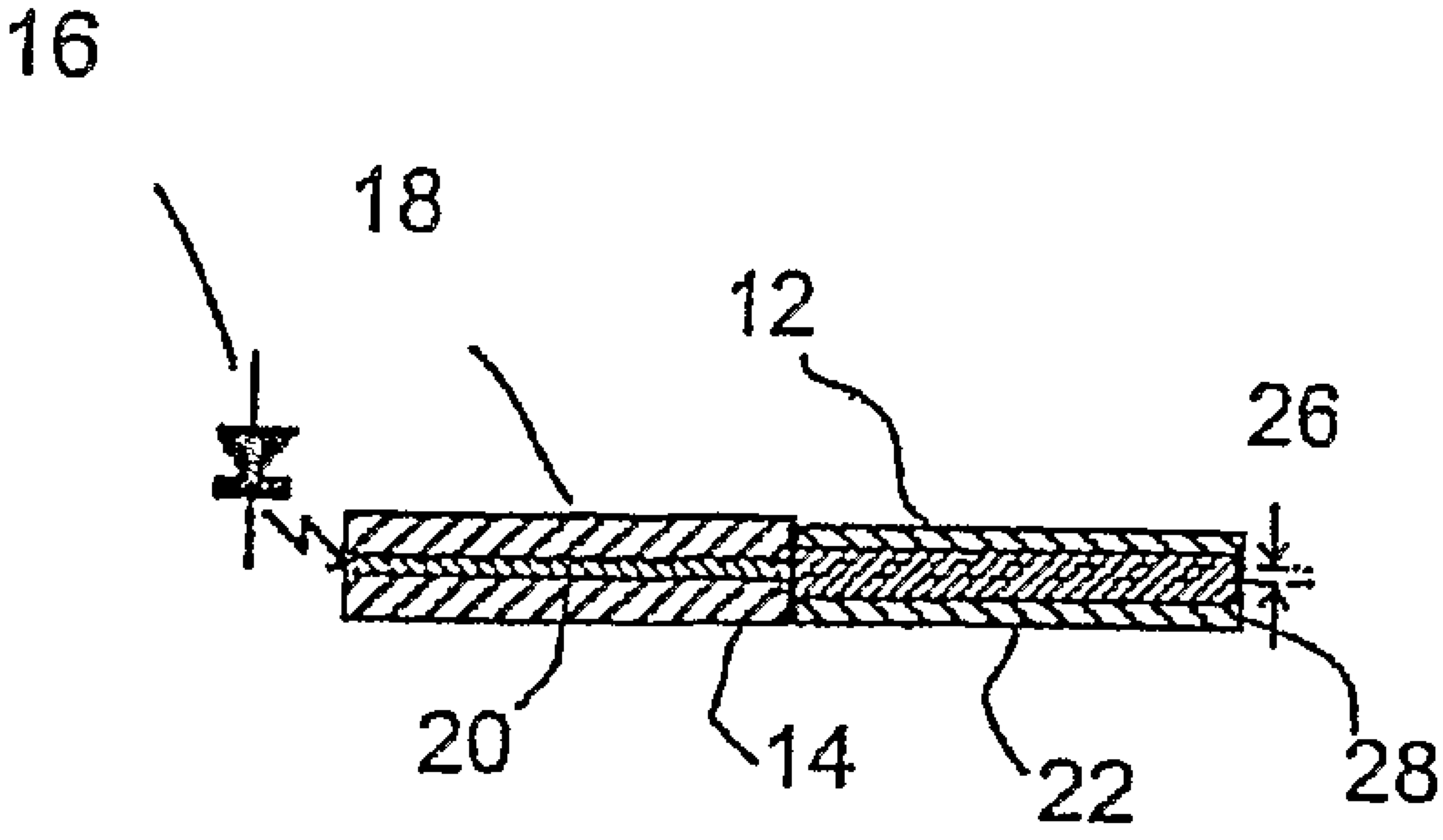

30
32
34
42
46
36
50
60
HIGH ORDER MODE OPTICAL COUPLER
OPTICAL DETECTION AND CONVERSION CIRCUITRY
BULK OPTICS OPTICAL COUPLER
OPTICAL DETECTION AND CONVERSION CIRCUITRY
PROCESSING CONTROL AND COMMUNICATION CIRCUITRY
INTERFACE CONNECTOR
40
52
54
58
44

FIG. 4


16
18
12
26
20
14
22
28