



- (51) International Patent Classification:
G02B 6/02 (2006.01)
- (21) International Application Number:
PCT/US2013/049458
- (22) International Filing Date:
5 July 2013 (05.07.2013)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:
61/668,110 5 July 2012 (05.07.2012) US
- (72) Inventors; and
- (71) Applicants : **HERBST, Brian** [US/US]; 107 Ascot Court, Easley, South Carolina 29642 (US). **DOBBINS, Patrick E.** [US/US]; 1000 Ansel School Road, Greer, South Carolina 29651 (US). **CIGNARALE, Joseph** [US/US]; 105 Rowland Court, Greer, South Carolina 29650 (US).
- (74) Agents: **PELLEGRINI, Carl J.** et al.; Sughrue Mion, PLLC, 2100 Pennsylvania Avenue, NW, Suite 800, Washington, District of Columbia 20037-3213 (US).

- (81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.
- (84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: TAMPER SENSITIVE FIBER OPTIC CABLE

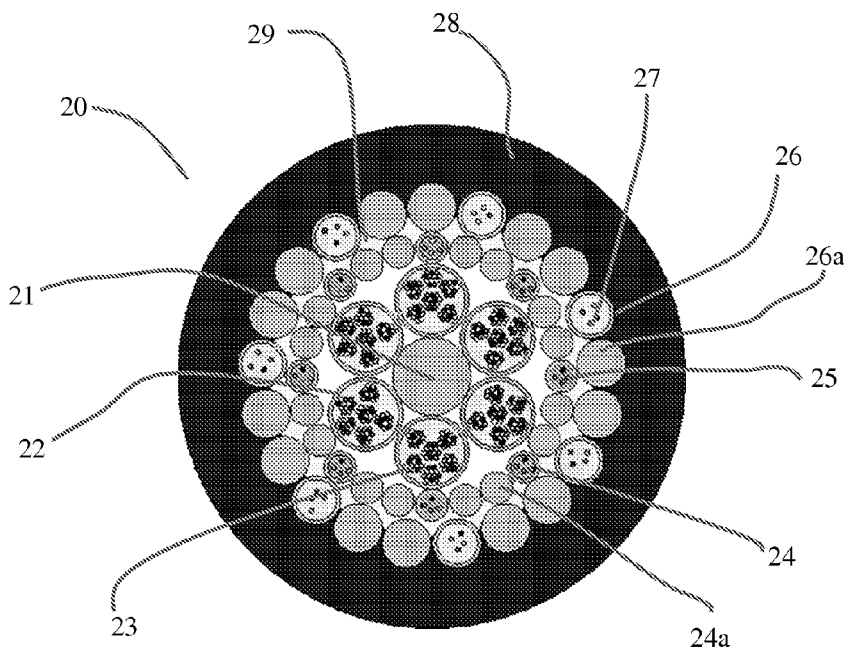


Figure 2

(57) Abstract: A fiber optic cable including an inner guard layer surrounding a core containing at least one optical fiber; and an outer guard layer surrounding the inner guard layer; wherein the inner guard layer includes at least one metal tube with at least one optical fiber inside the tube; and wherein the outer guard layer includes at least one metal tube with at least one optical fiber inside the tube.



Published:

- *without international search report and to be republished upon receipt of that report (Rule 48.2(g))*

TAMPER SENSITIVE FIBER OPTIC CABLE

CROSS-REFERENCE TO RELATED APPLICATIONS

[01] This application is based upon and claims the benefit of priority from United States Provisional Application No. 61/668,110, filed July 5, 2012, in the United States Patent and Trademark Office, the disclosures of which are incorporated herein in its entirety by reference.

BACKGROUND

1. Field

[02] The invention is related to a fiber optic cable, and more particularly to a highly tamper sensitive fiber optic cable.

2. Related Art and Background

[03] When optical fiber cables came into the market, it was deemed that they were tamper proof as someone could not tap into the core of the fiber to get to the data being transferred. Unfortunately, this is no longer true. The fiber can be tapped into to obtain the data that is being transmitted through splicing in a splitter or with a device that bends the fiber enough to create some leaking of the signal from the core. With the right equipment, this leaked signal can be captured.

[04] The need for secure communication is critical for a variety of entities ranging from the banking industry, government, military and industry. Typically the signals can be encrypted which improves the security but some risk remains as hackers are becoming more sophisticated.

[05] Therefore, there is a need for a system that can monitor if the cable is being tampered with. There are sophisticated interrogation systems that can measure vibration on an optical fiber using coherent Rayleigh processing or interferometric sensing technologies which also can measure vibration. If someone created vibration on a fiber optic cable while trying to access the fibers, these technologies would sense the event very well.

[06] However, if no vibration or minimal vibration was created, for example, by using chemicals/acids to eat away the cable structure to get to the communication fibers, the information being transferred could possibly be compromised. Therefore, there is a need to have a cable structure that can provide additional layers of tamper resistance.

SUMMARY

[07] Exemplary implementations of the present invention address at least the above problems and/or disadvantages and other disadvantages not described above. Also, the present invention is not required to overcome the disadvantages described above, and an exemplary implementation of the present invention may not overcome any of the problems listed above.

[08] One embodiment of the invention is a fiber optic cable with an inner guard layer surrounding a core containing at least one optical fiber; and an outer guard layer surrounding the inner guard layer; wherein the inner guard layer includes at least one metal tube with at least one optical fiber inside the tube; and wherein the outer guard layer includes at least one metal tube with at least one optical fiber inside the tube.

[09] Other features of the embodiment include the inner guard layer including a plurality of metal tubes with at least one optical fiber inside the plurality of metal tubes and the

outer guard layer includes a plurality of metal tubes with at least one optical fiber inside the plurality of metal tubes.

[10] Other features of the embodiment include the cable including a jacket surrounding the outer guard layer.

[11] Other features of the embodiment include the cable including a strength element in the core.

[12] Other features of the embodiment include the inner guard layer being wrapped in a helical pattern and the outer guard layer being wrapped in a contra-helical pattern.

[13] Other features of the embodiment include the cable including at least one of an adhesive and a polymer in spaces between at least one of the inner guard layer, the outer guard layer and the core.

[14] Other features of the embodiment include the cable including a plurality of the metal tubes in at least one of the inner guard layer and outer guard layer being welded together.

[15] Other features of the embodiment include the cable wherein a diameter of the inner guard layer metal tubes is different than a diameter of the outer guard layer metal tubes.

[16] Other features of the embodiment include the cable wherein a diameter of the inner guard layer metal tubes is smaller than a diameter of the outer guard layer metal tubes..

BRIEF DESCRIPTION OF THE DRAWING

[17] FIG. 1 is a cross-sectional view of an embodiment of a cable according to the present invention.

[18] FIG. 2 is a cross-sectional view of another embodiment of a cable according to the present invention.

[19] FIG. 3 is a side view of an embodiment of a cable according to the present invention.

DETAILED DESCRIPTION

[20] The following detailed description is provided to gain a comprehensive understanding of the methods, apparatuses and/or systems described herein. Various changes, modifications, and equivalents of the systems, apparatuses and/or methods described herein will suggest themselves to those of ordinary skill in the art. Descriptions of well-known functions and structures are omitted to enhance clarity and conciseness.

[21] Hereinafter, an exemplary embodiment will be described with reference to accompanying drawings.

[22] Referring to the drawings, FIG. 1 is a cross-sectional view of a cable 10 according to an exemplary embodiment of the invention. In this embodiment, cable 10 has the communication fibers 3 in the center of the cable. The exact core structure depends on the number of fibers being protected and may include a strength element 1 in the center. In this embodiment, the core structure includes five tubes 2 with sixteen optical fibers 3 in each tube 2. In various embodiments of the invention, the core structure could include, but not be limited to, fiber counts ranging from 1 to 3000. These optical fibers 3 would preferably be housed in a tube/structure 2 that is difficult to remove such as a stainless steel tube.

[23] Around the core is a layer of guard fiber elements 4 that may be wrapped in a helical pattern and over that is another layer of guard fiber elements 6 that may be wrapped contra-helically. FIG. 3 shows one possible wrapping pattern. In this figure, guard fiber elements 30 are wrapped helically and guard fiber elements 31 are wrapped contra-helically. The embodiment is not limited to two guard layers, and more could be added for improved tamper resistance. These guard fiber elements 4, 6 would house optical fibers 5, 7 and these would be interconnected and monitored optically by commonly known methods with the intent of looking for optical loss and/or acoustic/vibration signature. The intent is that if someone wanted to access the guard fibers 5, 7, they would have extreme difficulty getting through the two layers of guard elements 4, 6 without creating either optical loss or an acoustic/vibration signal.

[24] These guard elements would preferably be housed in a tube/structure 4, 6 that is difficult to remove such as a stainless steel tube.

[25] The outside of the cable could be covered by a jacket 8, made of known conventional cable jacket materials, including, but not limited to, polyethylene.

[26] In another embodiment, additional layers of polymers and adhesives between the layers, such as in spaces 9, can be added can make access to the communication fibers 3 increasingly difficult.

[27] In another embodiment, if metal tubes are used, the tubes may be spot welding together so they are not “un-stranded” easily.

[28] In another embodiment, if metal elements are used, an electric current can be driven through the structure and the current may be monitored. Thus, if part of the metal

structure is removed/cut, the signal will be disrupted, which would indicate possible tampering. Also, if metal elements are used, the resistance of the structure may be measured. Thus, if part of the metal structure is removed/cut, the resistance will change, which would indicate possible tampering.

[29] In another embodiment, the user may deploy decoy communication fibers in the core as well – i.e. using 432 fibers when they only need 48 fibers. They would transmit false data down the other fibers. Ideally the sequence would be adjusted randomly as well to create further difficulty to the entity trying to get into the key communication fibers.

[30] In another embodiment, polymer materials could be used to create a bond with the metal elements in the core. This both makes it more difficult to separate the elements and to identify the stainless tubes versus the wires.

[31] In another embodiment, decoy guard elements of stainless steel tube and/or thin walled polybutylene terephthalate (PBT) may be added to complicate the attempts to enter the cable.

[32] While the embodiment shown in FIG. 1 shows five tubes in the core, more or less tubes could be used depending on the size of the cable. Similarly, while eleven inner guard elements 4 are shown, more or less elements could be used depending on the size of the cable. Similarly, while seventeen outer inner guard elements 6 are shown, more or less elements could be used depending on the size of the cable. Likewise, while FIG. 1 shows that the inner guard elements 4 and outer guard elements 6 as having the same diameter, they could have different diameters, for example the diameter of the outer guard elements 6 could be larger than the diameter of the inner guard elements 4.

[33] While the embodiment shown in FIG. 1 shows fibers in each of the guard elements 4, 6, some of the guard elements can be left empty, be replaced with a filler component, rather than fibers, to reduce cost, or be made of a solid material/wire. However, to the outside, they would look just like the guard elements with fibers.

[34] In one preferred embodiment, the cable has a total of 492 fibers, which includes 72 fibers in each of six core tubes, which may be used for communications, and sixty guard fibers spread out in the inner and outer guard layers.

[35] Referring to the drawings, FIG. 2 is a cross-sectional view of a cable 20 according to another exemplary embodiment of the invention. This cable has a total of 492 fibers, which includes 72 fibers in each of six core tubes, which may be used for communications, and sixty guard fibers spread out in the inner and outer guard layers. In this embodiment, cable 20 has the communication fibers 23 in the center of the cable. The exact core structure depends on the number of fibers being protected and may include a strength element 21 in the center. In this embodiment, the core structure includes six tubes 22 with 72 optical fibers 23 in each tube 22. However, the core structure of this embodiment is not limited to these fiber counts. These optical fibers 23 would preferably be housed in a tube/structure 22 that is difficult to remove such as a stainless steel tube.

[36] Around the core is a layer of guard fiber elements 24 that may be wrapped in a helical pattern and over that is another layer of guard fiber elements 26 that may be wrapped contra-helically. See, for example. The embodiment is not limited to two guard layers, and more could be added for improved tamper resistance. These guard fiber elements 24, 26 would house optical fibers 25, 27 and these would be interconnected and monitored optically by

commonly known methods with the intent of looking for optical loss and/or acoustic/vibration signature. The intent is that if someone wanted to access the guard fibers 25, 27, they would have extreme difficulty getting through the two layers of guard elements 24, 26 without creating either optical loss or an acoustic/vibration signal.

[37] These guard elements would preferably be housed in a tube/structure 24, 26 that is difficult to remove such as a stainless steel tube. In this embodiment, decoy guard elements of stainless steel tube and/or thin walled polybutylene terephthalate (PBT) or solid materials/wires 24a, 26a may be added to complicate the attempts to enter the cable.

[38] The outside of the cable could be covered by a jacket 28, made of known conventional cable jacket materials, including, but not limited to, polyethylene.

[39] In another embodiment, additional layers of polymers and adhesives between the layers, such as in spaces 29, can be added can make access to the communication fibers 23 increasingly difficult.

[40] In another embodiment, if metal tubes are used, the tubes may be spot welding together so they are not “un-stranded” easily.

[41] In another embodiment, if metal elements are used, an electric current can be driven through the structure and the current may be monitored. Thus, if part of the metal structure is removed/cut, the signal will be disrupted, which would indicate possible tampering. Also, if metal elements are used, the resistance of the structure may be measured. Thus, if part of the metal structure is removed/cut, the resistance will change, which would indicate possible tampering.

[42] In another embodiment, the user may deploy decoy communication fibers in the core as well – i.e. using 432 fibers when they only need 48 fibers. They would transmit false data down the other fibers. Ideally the sequence would be adjusted randomly as well to create further difficulty to the entity trying to get into the key communication fibers.

[43] In another embodiment, polymer materials could be used to create a bond with the metal elements in the core. This both makes it more difficult to separate the elements and to identify the stainless tubes versus the wires.

[44] While the embodiment shown in FIG. 2 shows six tubes in the core, more or less tubes could be used depending on the size of the cable. Similarly, while 24 inner guard elements 24, 24a are shown, more or less elements could be used depending on the size of the cable. Similarly, while 21 outer inner guard elements 26, 26a are shown, more or less elements could be used depending on the size of the cable. Likewise, while FIG. 2 shows that the inner guard elements 24, 24a and outer guard elements 26, 26a as having the different diameters, they could have the same diameters.

[45] While the embodiment shown in FIG. 2 shows fibers in only some of the guard elements 24, 26, all of the guard elements could have fibers.

[46] As mentioned above, although the exemplary embodiments described above are various fiber optic cables, they are merely exemplary and the general inventive concept should not be limited thereto, and it could also apply to other types of cables.

LISTING OF CLAIMS

What is claimed:

1. A fiber optic cable, comprising:
an inner guard layer surrounding a core containing at least one optical fiber; and
an outer guard layer surrounding said inner guard layer;
wherein said inner guard layer includes at least one metal tube with at least one optical fiber inside said tube; and
wherein said outer guard layer includes at least one metal tube with at least one optical fiber inside said tube.

2. The cable of claim 1, wherein:
said inner guard layer includes a plurality of metal tubes with at least one optical fiber inside said plurality of metal tubes and
said outer guard layer includes a plurality of metal tubes with at least one optical fiber inside said plurality of metal tubes.

3. The cable of claim 2, further comprising a jacket surrounding said outer guard layer.

4. The cable of claim 2, further comprising a strength element in said core.

5. The cable of claim 1, wherein said inner guard layer is wrapped in a helical pattern and said outer guard layer is wrapped in a contra-helical pattern.
6. The cable of claim 2, wherein said inner guard layer is wrapped in a helical pattern and said outer guard layer is wrapped in a contra-helical pattern.
7. The cable of claim 1, further comprising at least one of an adhesive and a polymer in spaces between at least one of said inner guard layer, said outer guard layer and said core.
8. The cable of claim 2, wherein a plurality of said metal tubes in at least one of said inner guard layer and outer guard layer are welded together.
9. The cable of claim 1, wherein a diameter of said inner guard layer metal tubes is different than a diameter of said outer guard layer metal tubes.
10. The cable of claim 9, wherein a diameter of said inner guard layer metal tubes is smaller than a diameter of said outer guard layer metal tubes.

1/2

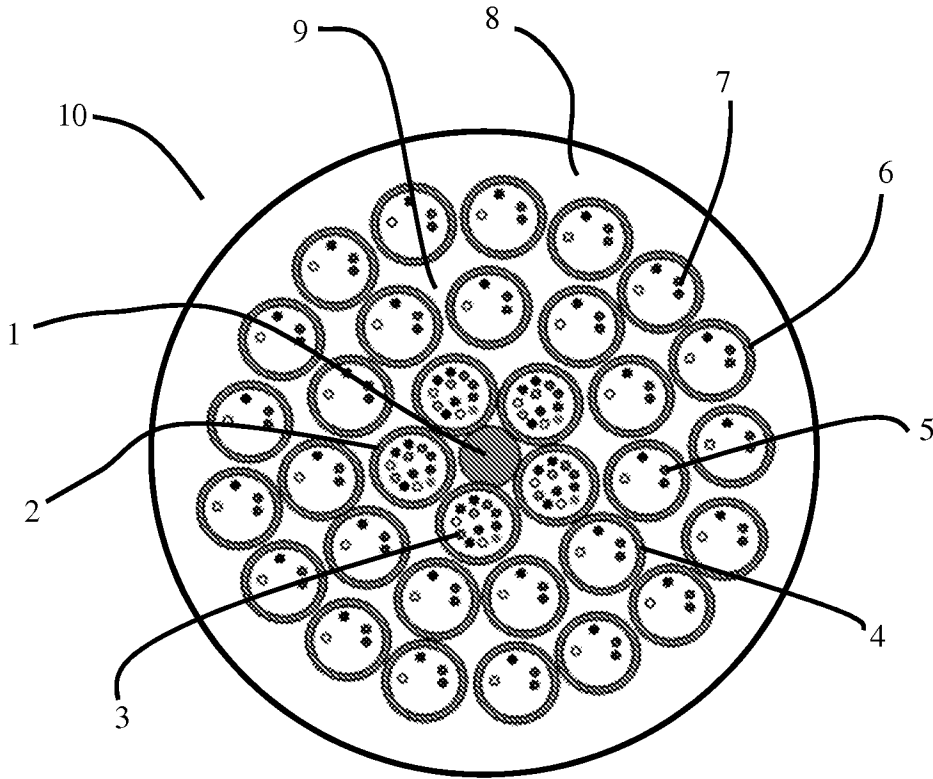


Figure 1

2/2

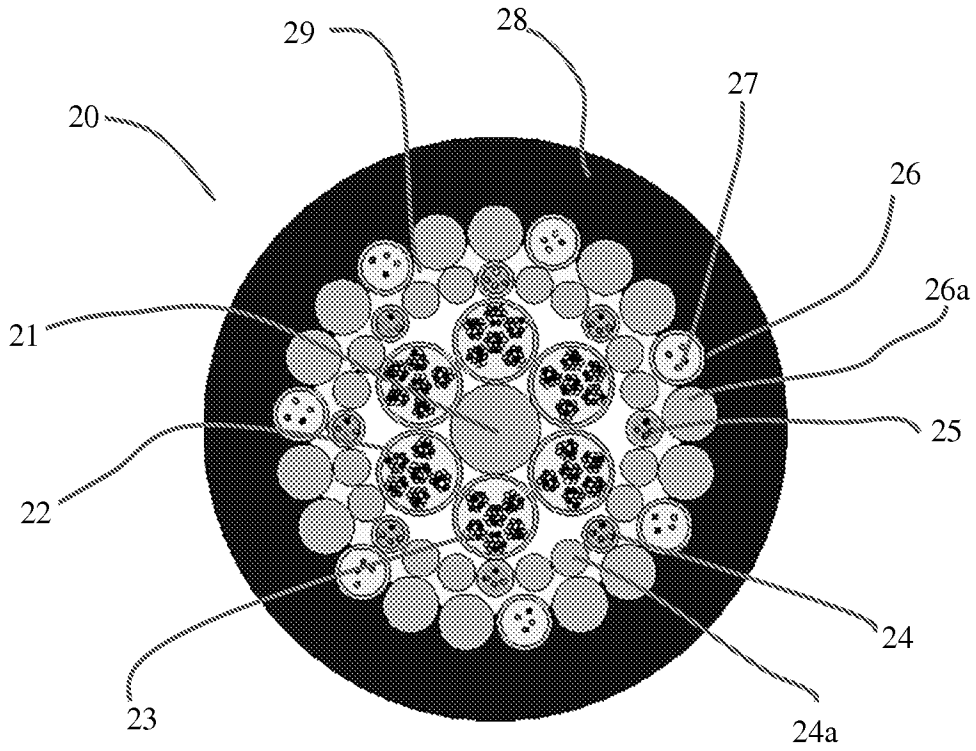


Figure 2

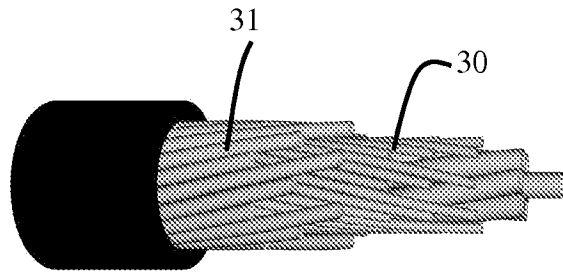


Figure 3