

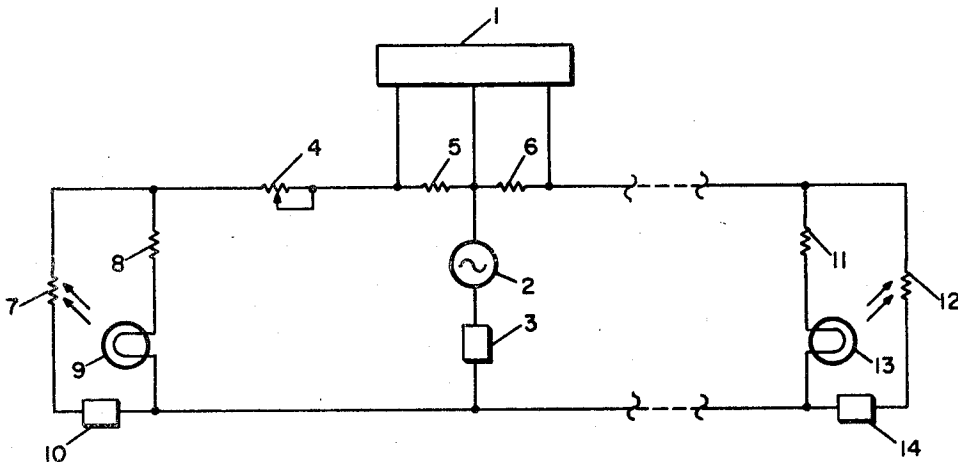
Sept. 9, 1969

C. S. MOOREFIELD

3,466,643

TRANSMISSION LINE TAMPERING ALARM SYSTEM

Filed March 18, 1966



INVENTOR.

CARLTON S. MOOREFIELD

BY *Carlton S. Moorefield*
Carlton S. Moorefield

1

3,466,643

TRANSMISSION LINE TAMPERING ALARM SYSTEM

Carlton Swain Moorefield, 4935 Birch Lane,
Alexandria, Va. 22312

Filed Mar. 18, 1966, Ser. No. 535,471

Int. Cl. G08b 21/00

U.S. Cl. 340—253

5 Claims

ABSTRACT OF THE DISCLOSURE

The present invention is a device for the protection of supervised conductors by utilizing an alarm means which is responsive to the non-tracking of a signal of two multi-mode non-linear matched modules. These elements track a random and dynamic signal and are themselves self adaptive in a tracking manner.

Summary of the invention

The purpose of petitioner's device is to supervise electrical conductors which are used to transmit a signal indicating the occurrence of a hostile act and to protect the circuit of both sensor and annunciator panel or to act as a protected line sensor and annunciator panel.

Most intrusion alarm systems indicate the occurrence of a hostile act through the use of electrical conductors to an annunciator panel. The hostile act itself is detected in many ways—ultra-sonic, radar doppler, magnetic switches, break-conductor, break contact, make contact, etc. Some systems permit the annunciator signal to occur at the point of the hostile act, others because of differing requirements have the signal indicating a hostile act appear at other points widely separated from the area of the hostile act sensor and place of hostile act. All systems which are very effective have some type of line supervision or system supervision to prevent tampering while in a protecting and non-protecting mode and this often includes the electrical conductors connecting the annunciator unit with the hostile act sensing unit.

Where a "rate of change" or "resistance" or "milli-ampere system" as they are often called are used as a means of line supervision or protection, it is just a matter of time until this system can be defeated by a hostile operator, since they yield to "voltage substitution," "resistance substitution" and other techniques within the means of a skilled operator.

One could envision a system employing very complicated cryptographic systems and computer programmed systems that would on a time base be tamper-proof. However the cost, complication of operation, and the need to have a system that will work with conductors having poor bandwidth handling capability, dictate a need for a simpler tamper-proof system. Another serious fault of most high security systems or those that respond to minute changes in conductor parameters, is the presence of a high false alarm rate.

One way to effect a system which would not yield to "voltage substitution" or "resistance substitution" or "element substitution" or other known countermeasure techniques, would be to effect a signal source at one end of the protected conductors and have matched elements at the signal source and at the opposite end of the protected conductor which react to this signal source in a tracking but non-linear manner. It would also achieve even greater security if this signal source were random in certain parameters. This would mean that the source could not be recorded, analyzed and with other parameters measured, then duplicated to effect a defeat of the system.

There is no intrinsic reason that some of the present cryptographic techniques could not achieve very high

2

security of supervision of the conductors if one could assume that cost, complication of equipment, space, and most important, conductor bandwidth handling ability, were not constraints upon the use of these intrusion alarm devices. The fact is that these matters do constitute very serious constraints upon the users of this type equipment. Consequently there is a very great need to achieve the same element of security of conductors and circuit supervision in an austere manner. That is the purpose of the device which is the subject of this petition.

Detailed description

The problem defined.—In considering this type of security device, you may assume that the opposition knows how the device works and most of its composition of parts. You may also assume he does not know the value of the parts. Because most systems exhibit some false alarms you must assume that the opposition has the ability to make voltage, current, and resistance and capacity measurements by causing two or three false alarms or perhaps without causing any alarms.

The attached drawing is an illustrative example of a device which would defeat the opposition even though he is granted all the previously made assumptions and advantages. This device employs a combination of a fixed resistance 8, a current dependent resistance such as an electroplating tube 10, a light dependent resistance 7, and a light source with fixed internal resistance 9 to form a module of elements with a non-linear resistance to the presence of a voltage. The non-linearity is due in part to the response time of the elements 9 and 7 and the action of 10—the second paired module at the opposite end of the protected conductors is composed of elements matched in value to the said first module and comprised of a fixed resistance 11, a light dependent resistance 12, a light source with fixed internal resistance 13, and a current dependent resistance 14. A means of matching the two modules or compensating for the resistance of the connecting line is accomplished by a variable resistor 4 series connected with the first module. It is possible that for extremely long and capacitive lines that it would be necessary to place a variable capacity in parallel with the first module to achieve proper matching and tracking; however, the inventor has not experienced the need for this on any units constructed and tested. To achieve even greater non-linearity or resistance to voltage in the module, a diode could supplement resistances 8 and 11. The inventor has used this successfully. The diodes are not shown on the drawings.

If the modules are tracking each other and reacting in the same non-linear way to the signal source 2 then the voltage drop across the two matched resistors 5 and 6 should be near equal. If something occurs to prevent one of the modules from tracking or reacting in the same manner as the other then a difference in voltage drop will occur across one of the matched resistors 5 and 6. This difference is detected in the drawing by a differential amplifier 1 which provides the means or voltage for sounding an alarm or whatever reaction is desired for the occurrence of an act which indicates tampering with the protected line.

The signal source 2 is any A.C. or D.C. voltage source whose amplitude is controlled by a unit 3. Unit 3 is a device, such as Scope Incorporated's audio color which converts acoustic energy into a voltage whose amplitude is dependent upon the intensity of the acoustic energy. In the present case the acoustic energy would be from a microphone detecting the energy in its environment. In the Scope Incorporated Audio Color device the voltage is controlled by a Hi-Fi set and the voltage is used to drive a set of colored lights.

The object of the combination of elements is to present a multimode non-linear reaction to the presence of voltage and voltage levels present on the protected conductors to present a changing and/or changeable multimode impedance.

The need for this becomes evident if one makes the assumptions of the knowledge that I have already made in the person performing the hostile act. It is easy to say, for instance, that if the person performing the hostile act can make a large number of electrical measurements on the protected lines or circuit, that by computer programming, he could achieve a combination of elements which would exhibit the same "transfer function" as the "module of elements" on the end of the protected line and thus substitute this in the line for the "module of elements" on the end of the line and defeat the system.

However, if on a time base the module of elements is changing, then by the time a "transfer function equivalent" could be worked out, even with computer speeds, the "module of elements" has adapted itself to a different and unknown multimode operation.

I claim:

1. An alarm system for signalling tampering with an electrical transmission line comprising:

first and second voltage dependent impedances, said first impedance being connected to one end of said transmission line, said first and second impedances having similar electrical characteristics, each impedance comprising means for converting electrical power into radiated power, and means responsive to said radiated power for further modifying the instantaneous value of the impedance;

a source of varying electric current, said source connected to said second impedance and the other end of said transmission line;

means for individually measuring a first current delivered by said source to said transmission line and a second current delivered by said source to said second impedance, and for comparing the instantaneous values of said first and second currents;

alarm means for indicating an inequality between said first and second currents representative of tampering with said transmission line.

2. The system of claim 1 further including means for adjusting the value of said second impedance to permit balancing of said first and second currents.

3. The system of claim 1, wherein said means for converting electrical power into radiated power is a light source, and said means responsive to said radiated power is a light dependent resistance.

4. The system of claim 1 wherein said first and second impedances further include an electroplating tube.

5. The system of claim 1 wherein said source of varying electric current is a voltage source in series with a microphone.

References Cited

UNITED STATES PATENTS

1,257,440	2/1918	Zehden	340—285
1,709,097	4/1929	Roe	340—276
1,870,181	8/1932	Mallory.	
2,217,797	10/1940	Donovan	340—233
3,029,420	4/1962	Bagno et al.	
3,060,417	10/1962	Blake.	
3,191,048	6/1965	Cowen	340—233 X

JOHN W. CALDWELL, Primary Examiner

D. L. TRAFTON, Assistant Examiner

U.S. Cl. X.R.

340—276, 285