Spring 3-1-1978

Conceptual Studies of intrusion Detection systems Using Leaky Transmission Lines

S W. Maley
University of Colorado Boulder

Scientific Report No. 30

CONCEPTUAL STUDIES OF INTRUSION DETECTION SYSTEMS USING LEAKY TRANSMISSION LINES

by

S. W. Maley

March 1978

This project is supported by the Deputy for Electronic Technology (RADC/ETEP), Hanscom AFB, Massachusetts 01731, under contract #F19628-77-C-0093.

Theory for a System Having a Single Intrusion Detection Zone

Intrusion detection systems can in general be characterized in terms of parameters such as the length, width, and shape of the detection zone, their ranging capability, and their sensitivity. In this analysis, the basic system in its simplest form is shown in Figure 1. The height, h, can be zero or negative. The transmission systems are coupled so that the receiver normally receives power coupled from the transmitting system into the receiving system. An intrusion into the region between the transmission systems will cause a variation of the power level into the receiver. The amount of variation depends upon the size and shape of the intrusion, its height above the ground and its orientation with respect to the transmission systems, the spacing d, the height h, and the length ℓ. To detect an intrusion with a high degree of confidence it is necessary that the receiver power level change by an adequate amount to serve as a definite and reliable indication of the intrusion. As a first approximation, it may be said that the relative change of power into the receiver is roughly proportional to the volume of the intrusion divided by the total volume within which intrusions are to be detected, or approximately

$$\text{relative change of power} \simeq \frac{\text{volume of intrusion}}{\ell d^2}$$

Here it is assumed that an intrusion can be detected up to a height about equal to the spacing of the transmission systems. Of course this rule is very rough because detectability depends upon the characteristics of the intursion and upon its height above the ground (since detectability in some configurations at least, decreases with the height of the intrusion); however the relationship gives a rule with which to explore

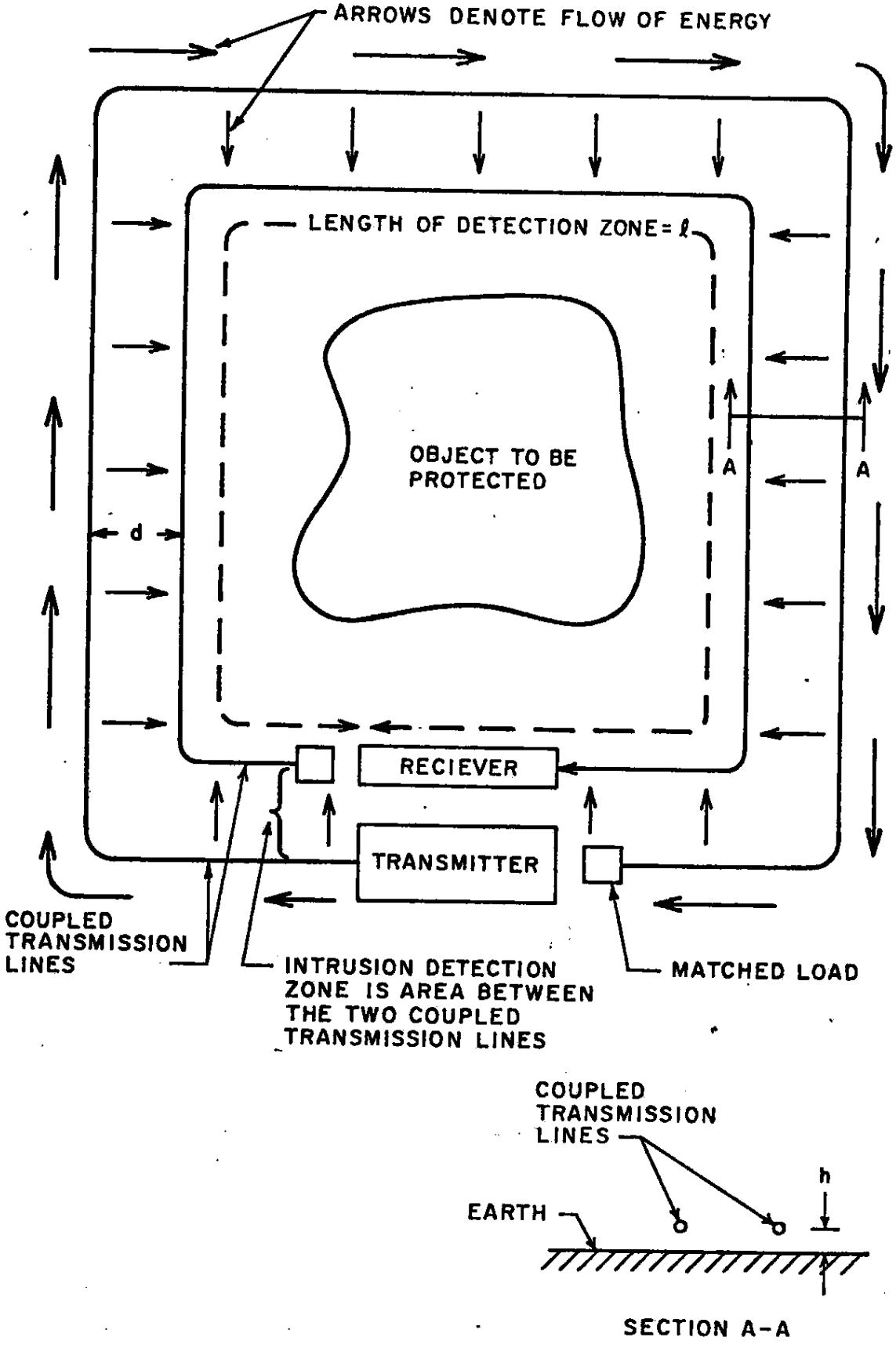

Fig. 1 BASIC INTRUSION SENSING SYSTEM

rather is dictated by the intended application. This then dictates that the overall system should be subdivided into short systems of such length as to give the required sensitivity in each section. The various sections are then operated independently. This complicates the system, but as will be discussed, the complication is not as severe as it appears at first thought and in addition the splitting up of the system into shorter lengths partially solves the problem of determining the location of the intrusion since the power will be monitored separately in the various sections.

Systems with Design Modification

The system as now proposed is sketched in Fig. 2. This diagram shows a transmitter and a receiver for each section but a variety of possibilities exist for various sections to share equipment. Some of these possibilities will be discussed now. Suppose there is one transmitter for each section and that each transmitter operates at a different frequency. Further suppose that there is only one receiving transmission system as shown in Fig. 3. The receiver could be tuned to each of the transmitter frequencies in sequence and then a signal level measurement could be made at each frequency. The measurements made at the various frequencies can then be used to detect an intrusion and to determine the section in which it occurred. Further possibilities for sharing of equipment will be discussed later.

This configuration can be modified so as to permit use of only one transmitter as shown in Fig. 4. In this configuration, each section is operated at a different frequency, just as in the configuration of Fig. 3, but in this case only one transmitter is used. The various sections of coupled transmission lines are fed through narrow band filters each having

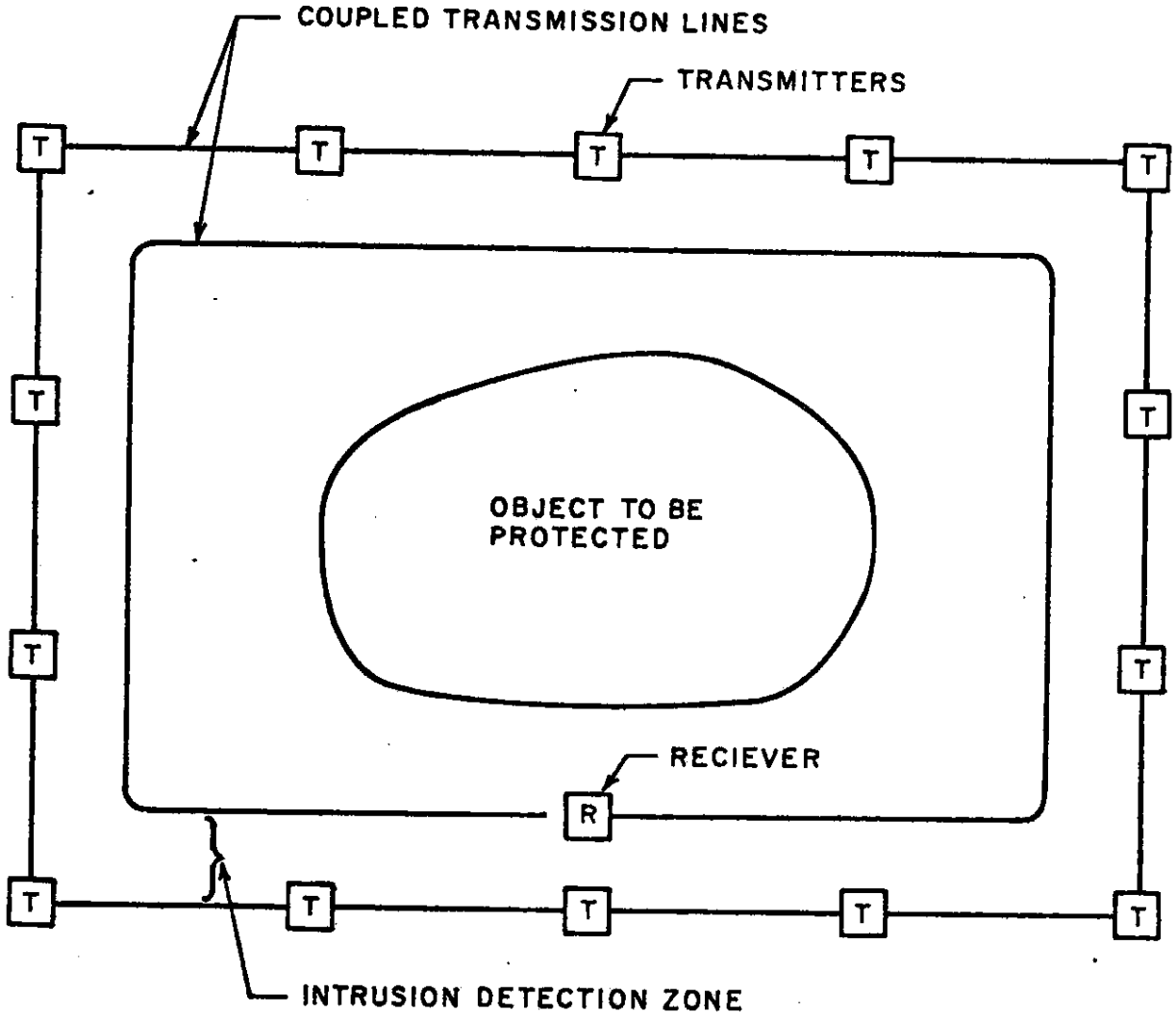

Fig. 3 MULTISECTION INTRUSION SENSING SYSTEM HAVING ONLY ONE RECIEVER

different non-overlapping frequency bands. The transmitter transmits a different frequency for each section for short periods of time in sequence. Thus the various sections operate one at a time in sequence. The sequence that the system goes through can be fast so that there is no chance of an intrusion that cannot be detected. The transmitter could be a variable frequency signal generator that steps through a sequence of discrete frequencies or perhaps it could be a sweep generator. The receiver could be the same as used in the configuration shown in Fig. 3 above in which each section has a separate transmitter on a different frequency. In operation the receiver makes signal measurements at the time each of the various frequencies is transmitted by the transmitter. Thus the timing within a cycle of measurements at which a change of signal is sensed indicates the section in which an intrusion has occurred.

In the application of the system such as described above, if it is necessary to decrease the probability of false alarms, then two systems could be used. One system could be completely outside the perimeter of the other or alternatively one could be completely within the detection zone of the other. The detection of intrusions by the two systems could be coordinated so that an intrusion alarm would occur only if both systems detect an intrusion at the same time in the same place. Such a compound system could greatly diminish the probability of a false alarm. This, however, may result in an unacceptable probability of an undetected intrusion. In that case three systems may be used so that an alarm occurs when 2 or more of the 3 systems detect an intrusion. In general it can be said that the use of multiple systems permits the probabilities of the various type of errors to be reduced to acceptable

levels. An alternative system design substituting discrete transmitting and receiving elements for the coupled transmission lines has some advantages in some applications. Such a design is discussed in the Appendix.

A system of the type described in the previous section can be synthesized using components many of which are off-the-shelf items. It will be necessary to determine, experimentally, an appropriate frequency band to use. This can be investigated experimentally or theoretically. Probably the wavelength should be comparable to the dimensions of the intrusions to be detected. The availability of frequency assignments will be an important consideration in selection of frequencies. Most of the other components of the system can be purchased. The transmission lines could be selected from a number of such lines that are commercially available. The transmitters could be fixed-frequency signal generators for the system using multiple transmitters or it could be a frequency synthesizer or a sweep generator for the other system discussed in the previous section. The receiver for the system having one receiver but separate transmitters for each section would have to be tunable. However, for the system having only one transmitter which steps in frequency, it could be simply a detector with a digital voltmeter to measure its output. This type would also be satisfactory for the system having separate receivers and transmitters for each section.

Signal Processing Aspects of System Design

The intrusion sensing system should be designed to operate under computer control. A microprocessor could probably be used to control

a number of such systems. The receiver, under computer control, must make measurements of signal level for each of the sections of the system in sequence. The result of each measurement should be stored by the computer for comparison with previous measurements for the same section and for other processing as required for the detection of intrusions. In operation, the system will make repeated measurements of the received signal strength in each section of the system. There may be many measurements for each section each second. These measurements will be stored in the memory of the computer as diagramatically suggested in Table I. The data given suggests no intrusions in sections 1, 3, and 4 because the signal measurements change by only small amounts from one measurement to the next. The small variations will be due to various types of noise in the system. These changes will be disregarded. However there appears to be an intrusion in section 2 because of the abrupt, large change in measurements at the receiver.

The computer must be programmed to examine these sequences of measurements in each section and to give an alarm when an intrusion is apparent. The examination of the pattern of measurements could be done in a variety of ways. The procedure could be such as to permit slow changes in the level of measurements as may occur due to changes in temperature, humidity, or when the ground becomes wet and to give an alarm only for large abrupt changes. If two systems were in use to protect the same area, then an alarm should be given only if both systems detect an intrusion at the same time in the same place (this gives protection against false alarms). A change in the procedure for detecting intrusions from the measurements stored in the computer memory can be accomplished by changing the program of the computer.

Table No. 1

Time Interval	Power Measurement Section 1	Power Measurement Section 2	Power Measurement Section 3	Power Measurement Sectiom 4
1	0342	0421	0393	0511
2	0344	0422	0394	0510
3	0339	0419	0395	0510
4	0340	0425	0395	0514
5	0338	0499	0397	0512
6	0338	0502	0396	0511
7	0343	0509	0399	0515
.	.	.	.	.
.	.	.	.	.
.	.	.	.	.

The set of measurements from the receiver during one cycle of the sequence is the set of numbers in one of the rows of Table I. This set of numbers characterizes the region between the two transmission systems at a particular time, and it may be referred to as a signature. The signature is a collection of side-by-side numbers, each number consisting of several digits and each of these numbers may change by small amounts from one cycle to the next, that is from one signature to the next, but such changes will be called insignificant signature changes. However, when an intrusion occurs in one of the sections, then one of the numbers (consisting of several side-by-side digits) in the signature will change by a large amount (the system is assumed to be designed with a sufficient number of sections that the smallest object to be detected will produce an unmistakenly large change in the appropriate number of the signature). This could be called a significant change in the signature. An intrusion alarm should be given when significant changes in the signature occur. The monitoring of the signature as done by the computer may be referred to as signature analysis. A normal signature, that is, the signature when no intrusion is present, can be determined when the system is put into operation. Normal signatures will be different for different conditions of weather, ground moisture, etc. Signature changes due to environmental changes may be substantial, but these changes will occur slowly since environmental conditions change slowly. Therefore it should not be difficult to distinguish environmental changes from an intrusion by signature analysis performed by the computer. The signature analysis program can be written in such a way as to continuously update the normal signature (the signature with no intrusion present) as environmental conditions change but to give an intrusion alarm when abrupt changes occur.

Some research and experimentation needs to be done to determine the best procedure for signature analysis. It should be noted that signature analysis requirements may be different for different applications.

The diagram of the system as now proposed is shown in Fig. 5. The micro-processor controls the stepping of the transmitter through the proper sequence of frequencies. (This is unnecessary if the system with multiple fixed frequency transmitters is used.) It also controls the receiver so as to make a measurement at each frequency. The output of the receiver is digital and is stored by the computer so as to make up a signature once for each cycle of measurements. The computer then performs signature analysis and sounds an alarm and gives the location of the intrusion when intrusions occur.

System Development

The development of the system described in the previous section will require some investigation of the characteristics of available leaky coaxial cable. The coupling circuits and filters can probably be off-the-shelf items, or if new designs are needed, they apparently will be simple design problems. The problem of connecting many circuits to a single transmission line will also require some investigation. One possible course of action would involve the use of coaxial cable and connectors of the type used by the CATV industry. The cable has low loss making long cable runs practical and the connectors to couple the filters to the cable are of the type that makes the connection to the coaxial cable without the necessity of cutting it or inserting any fittings. Furthermore it is relatively easy to move a coaxial cable tap from one location to another. The power level in the system should be made sufficiently high that receivers need not have any

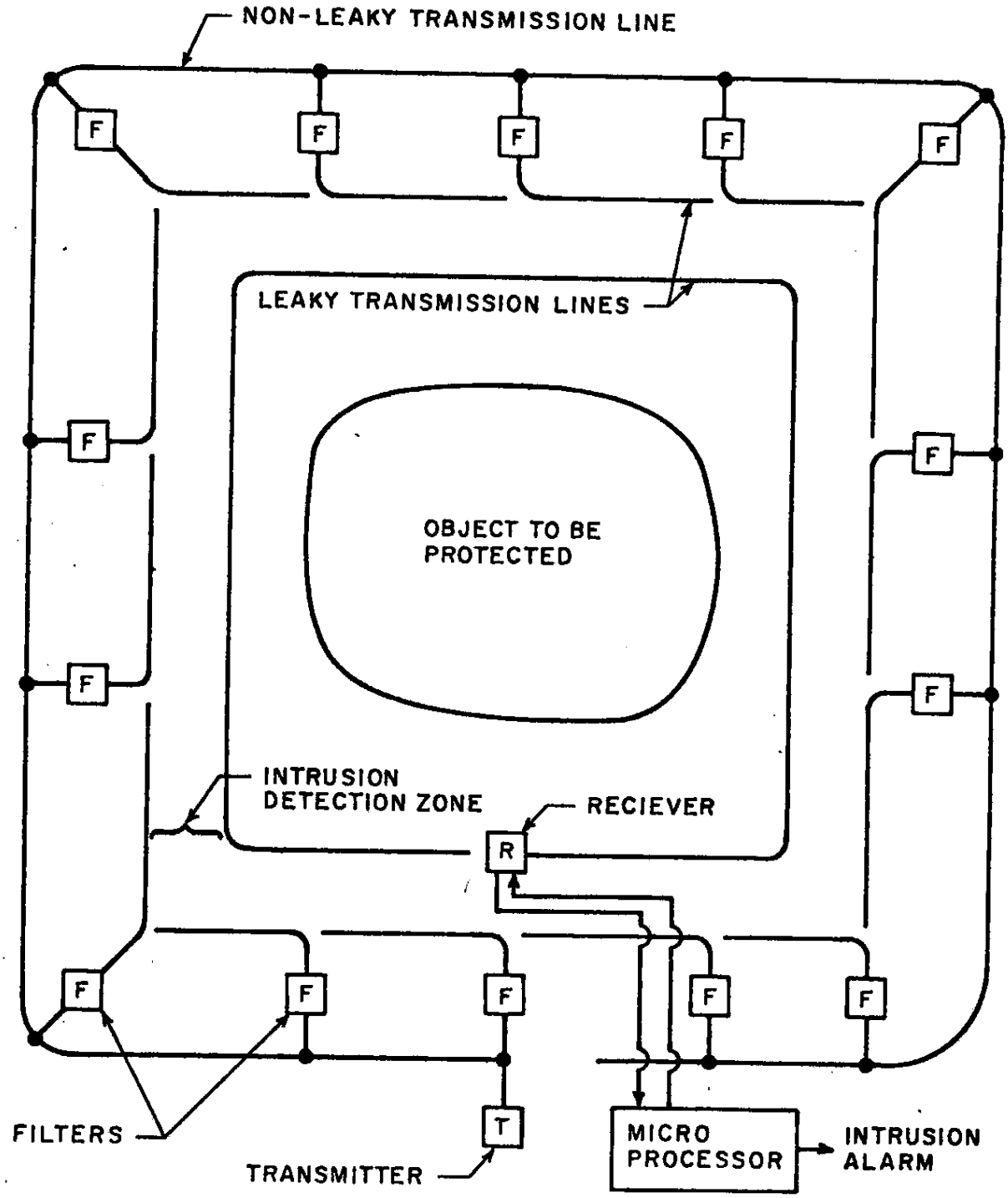

Fig 5 A COMPUTER CONTROLLED INTRUSION DETECTION SYSTEM

amplifiers. The untuned receivers can be of a type consisting of simply a detector and a digital voltmeter. The voltmeter should be capable of computer control. There are a number of such digital voltmeters commercially available. After the system has been adequately developed and tested, it may be possible to substitute a less expensive computer controlled analog-to-digital converter for the digital voltmeter. The type of transmitter to be used depends on the choice of transmission system. If the system is chosen to be the one having separate fixed frequency transmitters for each section, then there are a number of commercial devices available for use. If the system using one transmitter is selected, it must be capable of frequency stepping or sweeping on command from a microprocessor. There are a number of such sweep oscillators and frequency synthesizers available commercially. The microprocessor control system could be any of a variety of types now available. The program to control the transmitter (if needed) and to control the receiver and store receiver output so as to make up signatures, is a straightforward and rather simple programming job. The program for signature analysis to detect intrusions will require some research, development and test. Furthermore different applications may require signature analysis procedures that are different. It may be expected that after some systems have been developed and tested, the microprocessors for other systems for similar applications, can be simply supplied with a dedicated program in read-only memory.

APPENDIX

An Intrusion Sensing System Having Discrete Radiating Elements

The starting point for this discussion is the proposed system shown in Figure 3.

Consider the nature of the coupled transmission systems. They could consist of two leaky transmission lines. The power that leaky transmission lines radiate is governed by their design, by the characteristics of the earth and by the proximity of the transmission lines to the earth. It appears that such transmission lines could be designed for a variety of applications. But it also appears that different designs would be needed for different detection zone widths for different transmission system heights for different earth parameters and for systems of differing sensitivities. This necessity, for a variety of different transmission line designs, is undesirable from the point of view of adapting the system to different applications and from the point of view of maintenance. An alternative approach would be the use of a non-leaky transmission line with radiating structures (antennas) connected to both the transmitting and receiving systems at periodic intervals. This approach necessitates the design of antennas for various applications but it appears that fewer different designs will be needed and each design will be adaptable to a number of applications. This approach gives the system designer the opportunity to use any of a selection of antenna designs with various circuits for coupling them to the transmission lines and with any of a range of spacings of the antennas

along the transmission lines in order to control the detection zone width and shape, to compensate for differing heights of the radiating system with respect to the ground surface, and for various earth parameters and to control radiated power levels. The system as now proposed is as sketched in Fig. A1. In this sketch there are shown three antennas per section along the length. (A section is defined here as a length within which all antennas are excited at the same time and at the same frequency.) The number could vary from one up to several depending upon the requirements for sensitivity, the width of the detection zone, and the requirements on the accuracy of the location of the intrusions to be sensed. This system shown in Figure A1 can be adapted to the use of a single transmitter in the same way as was done previously; this is shown in Figure A2.

The systems discussed in this Appendix are adaptable to use in combinations of two or more with the objective of reducing the probability of false alarms, just as was discussed in the section on theory.

The design and development of the system described in this Appendix involves the same problems as for the system discussed previously with the additional problem of design of the discrete radiating elements.

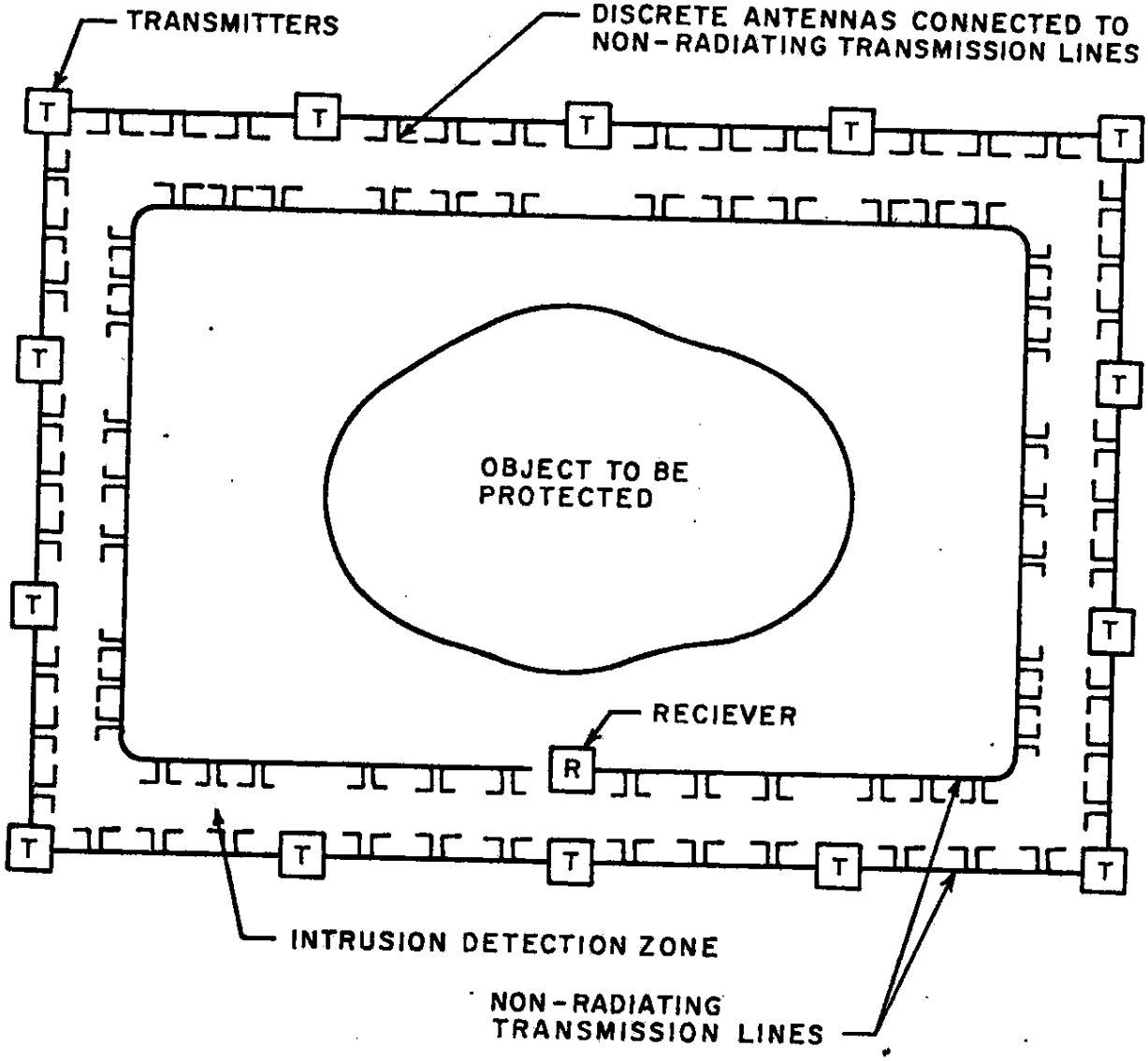

Fig A1 A MUTHSECTION INTRUSION SENSING SYSTEM USING DISCRETE ANTENNAS RATHER THAN COUPLED TRANSMISSION LINES

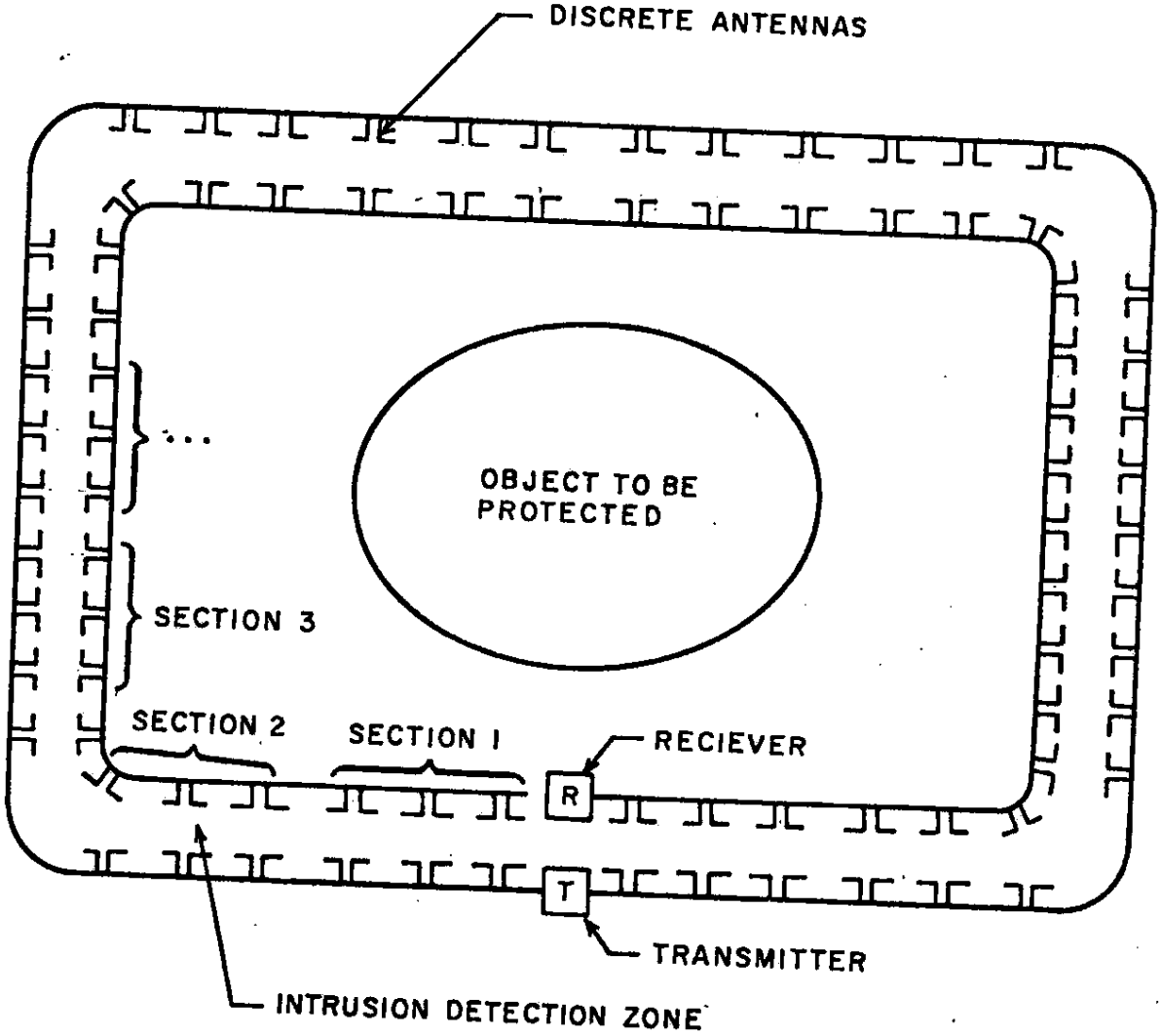

Fig A2 A MULTISECTION INTRUSION SENSING USING DISCRETE ANTENNAS BUT HAVING ONLY ONE RECIEVER AND ONE TRANSMITTER

References

1. An RF Intrusion Sensor for Isolated Resources, Nicholas V. Karras, Peter R. Franchi, Ronald L. Fante, J. Leon Poirier, Report RADC-TR-77-118, Rome Air Development Center, Air Force Systems Command, Griffis Air Force Base, New York, 13441, March 1977, 31 pp.

2. A High Resolution Guided Radar System, N.A. Mackay, D.G. Beattie, Electronic Letters, vol. 12, no. 22, pp. 583-4, 28 Oct. 1976.

3. A High Sensitivity Narrow Band Time Domain Reflectometer, Nielson A.M. Mackay, Sidney R. Penstone, IEEE Trans., vol. IM-23, No. 2, pp. 155-8, June 1974.

4. A Guided Radar System for Obstacle Detection, R.E. Patterson, Nielson A.M. Mackay, IEEE Trans., vol. IM-26, no. 2, June 1977.