CLAIMS

1.- An intrusion detection system (1), the system (1) comprising:

- at least one mesh surface (2), each mesh surface (2) comprising at least two cells (3), each cell (3) comprising a pattern (20), a pattern (20) being a portion of continuous electrical circuit,

- at least one interconnection surface (4) comprising a plurality of connectors (24), the connectors (24) being suitable for connecting cells (3) of the mesh surface(s) (2) to each other according to a first configuration of the interconnection surface (4) for forming groups of electrically connected cells (3), the patterns (20) of the cells (3) of each group forming a continuous electrical circuit of patterns (20),

- a detection module (8) able to detect a modification of an impedance which is characteristic of each group of electrically connected cells,

characterized in that the system (1) further comprises a configuration module (6) for configuring interconnections of the connectors (24), the configuration module (6) being able to modify, over time, the first configuration to obtain at least one second configuration of the interconnection surface (4), and the configuration module (6) being able to modify the configuration of the interconnection surface (1) when an intrusion attempt is detected by the detection module (8).

2.- The system (1) according to claim 1, wherein the configuration module (6) is able to determine, randomly, the second configuration from among a plurality of configurations of the interconnection surface (4) and to reconfigure the set of interconnections of the connectors (24) according to the second configuration.

3.- The system (1) according to any one of claims 1 to 2, wherein when a break in the electrical continuity of at least one continuous circuit is detected over an area of a mesh surface (2), the configuration module (6) is able to modify the configuration of the interconnection surface (4) so as to increase the number of groups of connected cells present in that area.

4.- The system (1) according to any one of claims 1 to 3, wherein the system (1) comprises at least two mesh surfaces (2) and a module for measuring variations in a property between two of the mesh surfaces (2), the property being chosen from among an impedance, a resistance, a capacitance and an inductance.

5.- The system (1) according to any one of claims 1 to 4, wherein at least one electrical circuit is formed by the connection, which is not reconfigurable by the configuration module (6), of at least two adjacent cells (3) of a mesh surface (2) via a component previously statically configured.

6.- The system (1) according to any one of claims 1 to 5, wherein the configuration module (6) is able to move over time, over one or over each mesh surface (2), a zone of the mesh surface (2) having the highest number of groups of connected cells.

7.- The system (1) according to any one of claims 1 to 6, wherein the system (1) comprises a member able to activate, at randomly or pseudo-randomly chosen moments, the configuration module (6) and/or the detection module (8).

8.- The system (1) according to any one of claims 1 to 7, wherein the interconnection surface (4) comprises a programmable component, the configuration module (6) and the detection module (8) being software applications integrated into the programmable component.

9.- The system (1) according to any one of claims 1 to 8, wherein the interconnection surface (4) comprises a micro-electromechanical system piloted by actuators, the configuration module (6) being able to actuate the actuators.

10.- The system (1) according to any one of claims 1 to 9, wherein the mesh surface (2) and the interconnection surface (4) form a physical protective barrier for the configuration module (6) and the detection module (8).

11.- The system (1) according to any one of claims 1 to 10, wherein, after a break has been detected in the electrical continuity of a group of connected cells, the detection module (8) is able to apply a security policy, the security policy comprising erasing sensitive data, carrying out integrity tests and/or reconfiguring interconnections of the connectors (24) of the interconnection surface (4).

12.- The system (1) according to any one of claims 1 to 11, wherein the detection module (8) includes several methods for detecting a break or alteration of each group of electrically connected cells and is able to use them in a combined manner with a defined temporal interleaving, which may be pseudo-random or random.

13.- An intrusion detection method, the method comprising the following steps:

- providing (100) a system (1) for detecting intrusions according to any one of claims 1 to 12,

- determining (110), using the configuration module (6), a first configuration of the interconnection surface (4),

- configuring (120), using the configuration module (6), interconnections of the connectors (24) of the interconnection surface (4) according to the first determined configuration,

- activating (130) the detection module (8) to detect a modification of an impedance which is characteristic of each group of electrically connected cells,

- optionally detecting (140), via the detection module (8), a modification of an impedance which is characteristic of a group of electrically connected cells, and

- modifying the first configuration of the interconnection surface (4), using the configuration module (6), to interconnect the connectors (24) of the interconnection surface (4) according to a second configuration.