International Journal of Technical Research and Applications e-ISSN: 2320-8163,
www.ijtra.com Volume 3, Issue 2 (Mar-Apr 2015), PP. 109-116

THE THREE DIMENSION-BASED PHYSICAL ACCESS CONTROL DETECTION SYSTEM, THE NATURE, THE LOCATION, AND THE TIME

Dr. M. Amer shedid[1], Ass. Prof. Magdy E. Elhennawy[2]
[1]The Future Higher Institute for Specialized Technological Studies
Computer Science Dept., Future Academy,
[2]High Institute of Computers and Information Technology,
Computer Dept., El-Shorouk Academy,
Family Card Project Consultant, Cairo, Egypt,
[1]mo_amer2002@yahoo.com, [2]mhennawy@ad.gov.eg

Abstract:- In fact, the application of physical security as to pass or prohibit pass is satisfactory for a variety of applications, but it is inappropriate for specific applications. The areas that need to be surveyed without interaction of human is one example. The fields and areas which are subjective to territory activities is another example. In many places in the world, bombing can explode buildings, lives, facilities, and so many others. In such cases we need to manage the situation remotely. We need a physical access control detection system that can survey the field without human direct intervention. Such system can intervene electronically to detect the parameters needed to decide the appropriate actions.

In this paper, a new approach for providing the parameters needed for decision maker, in such situations, is presented, it is the three dimension-based physical access control detection system, with the parameters; the nature, the location, and the time. The approach depends on defining three parameters, which are the nature of the passing object, the location of the object in the protected area, and the time in which the object is placed in that location. This approach depends basically on the sensor network and immune system combined with a central system that can receives a signal with such parameters to allow decision maker enough information for decision making. The new approach has been presented including the capabilities and architecture.

I. INTRODUCTION

Physical security is concerned with the protection against unauthorized physical access. It intended to deter, detect, and monitor/record intruders and trigger appropriate incident responses (e.g. by security guards and police).

Various methods, on the other hand, for physical access control may be applied. Access control may include mechanical access control systems, electronic access control systems, or identification systems and access policies. Intrusion detection and electronic surveillance may include alarm systems and sensors, or video surveillance. One of the basic methods is the physical access control gates. It is designed in such a way that it has a sensor that senses the mal materials during the object passing the gate.

One of the critical threats, today's, is the accessing of a prohibited area and leaves a mal object or mal material such as ammunition or explosive material, as happened in the terrorism situations executed by terrorisms.

One of the new approaches that can be appropriate for achieving the physical access controls is the wireless sensor network in which a set of sensors are distributed on a specific area to form a network organized and cooperated together. Such sensor network can be connected to a central station to communicate and process received signals from such network about any mal object accessing the specified area **[1, 2].**

Meanwhile, Artificial Immune Systems (AIS) are adaptive systems inspired by theoretical immunology and observed immune functions, principles and models, which are applied to complex problem domains. Artificial Immune Systems (AIS) emerged in the 1990s as a new branch in Computational Intelligence (CI).A number of AIS models exist, and they are used in pattern recognition, fault detection, computer security, and a variety of other applications researchers are exploring in the field of science and engineering **[3].**

In this paper, the introduction is mentioned in section one, this section. An overview about the physical access control gates is presented in section two. In section three the current state of the art of the physical security and access control systems is presented in addition to sensor network and immune system. In section four, the already existing system's drawback is stated. The approach of the three dimension-based physical access control gate is presented in section five. The results of case implementation are stated in section six. The conclusions and future work is mentioned in section seven and eight.

II. OVERVIEW

The term access control refers to the practice of restricting entrance to a property, a building, or a room to authorized persons. Physical access control can be achieved by a human (a guard, bouncer, or receptionist), through mechanical means such as locks and keys, or through technological means such as access control systems like the mantrap. The structure of the already existing access control gate allows, only, giving one fact; it is to grant pass or prohibit pass. The employed sensor designates the mal material, and signals the system which decides to pas or not to pass.

Now, a variety of access control gate types are available with the application of physical security. For an object passing through the gate, it allows to pass or prohibit pass, which is, for now, satisfactory for some of applications. Meanwhile, it is inappropriate for specific applications such as territory activities and the areas that need to surveyed without interference of human. In many places in the world, bombing can explode buildings, lives, facilities, and so many others. In

such cases we need to manage the situation remotely. We need a physical access control system that can survey the field without human direct intervention. Such system can intervene electronically to detect the parameters needed to decide the appropriate actions. The proposed system presented in this paper defines the parameters that are needed to the decision maker to manage the above situation. It is by defining the nature of the object passing the protected area, the location in absolute coordinates, and the time of accessing that area.

III. CURRENT STATE OF THE ART

A. Physical Security

Physical security describes security measures that are designed to deny unauthorized access to facilities, equipment and resources, and to protect personnel and property from damage or harm [**4**]. Physical security involves the use of multiple layers of interdependent systems which include CCTV surveillance, security guards, protective barriers, locks, access control protocols, and many others. Physical security systems for protected facilities are generally intended to:[**5,6.7**] deter potential intruders; detect intrusions and monitor/record intruders; and trigger appropriate incident responses.

It is up to security designers, architects and analysts to balance security controls against risks, taking into account the costs of specifying, developing, testing, implementing, using, managing, monitoring and maintaining the controls, along with broader issues such as aesthetics, human rights, and health and safety. Physical access security measures that are appropriate for a high security prison or a military site may be inappropriate in an office, a home or a vehicle, although the principles are similar.

Design of physical security system depends on the needs, nature and constituted elements of that system. Methods of physical security can be classified into more than one method. Deterrence methods may include physical barriers, natural surveillance, and security lighting. The initial layer of security for a campus, building, office, or other physical space uses crime prevention through environmental design to deter threats. Some of the most common examples are also the most basic: warning signs or window stickers, fences, vehicle barriers, vehicle height-restrictors, restricted access points, security lighting and trenches [**8, 9.10.11**].

Intrusion detection and electronic surveillance may include alarm systems and sensors, or video surveillance. Alarm systems can be installed to alert security personnel when unauthorized access is attempted. Alarm systems work in tandem with physical barriers, mechanical systems, and security guards, serving to trigger a response when these other forms of security have been breached. They consist of sensors including motion sensors, contact sensors, and glass break detectors [**12**]. However, alarms are only useful if there is a prompt response when they are triggered. Security personnel are common element in most of such method. Access control methods are used to monitor and control traffic through specific access points and areas of the secure facility. This is done using a variety of systems including CCTV surveillance, identification cards, security guards, and electronic/mechanical control systems such as locks, doors, and gates.[**13, 14, 15**]

B. Survey to Access Control Systems Operational Aspects

Several physical access control systems exist; examples are control panel-based access control, physical access control gates, and others. When a credential is presented to a reader, the reader sends the credential's information to a control panel, a highly reliable processor. The control panel compares the credential to an access control list, grants or denies the presented request, and sends a transaction log to a database. If there is a match between the credential and the access control list, the control panel operates a relay that in turn unlocks the door.

The electronic access control system grants access based on the credential presented. When access is granted, the door is unlocked for a predetermined time and the transaction is recorded. When access is refused, the door remains locked and the attempted access is recorded. The system will also monitor the door and alarm if the door is forced open or held open too long after being unlocked.

The above description illustrates a single factor transaction. Credentials can be passed around, thus subverting the access control list. To prevent this, two-factor authentication can be used. In a two factor transaction, the presented credential and a second factor are needed for access to be granted; another factor can be a PIN, a second credential, operator intervention, or a biometric input.

A credential is a physical/tangible object, a piece of knowledge, or a facet of a person's physical being, that enables an individual access to a given physical facility or computer-based information system. Typically, credentials can be something a person knows (such as a number or PIN), something they have (such as an access badge), something they are (such as a biometric feature) or some combination of these items. This is known as multi-factor authentication. Biometric technologies, on the other hand, include fingerprint, facial recognition, iris recognition, retinal scan, voice, and hand geometry **[16, 17**].

C. Wireless Sensor Networks

A wireless sensor network (WSN) is a sophisticated system that links the physical world with digital data networks. Wireless sensor networking is an emerging technology that has a wide range of potential applications including environment monitoring, smart spaces, medical systems and robotic exploration. Sensor network research is primarily driven by military applications such as battle-field surveillance and enemy tracking, where it provides the ability for the detection and tracking of enemy soldiers and their vehicles [**18**].

A wireless sensor network (WSN) generally consists of a base station (or gateway) that can communicate with a number of wireless sensors via a radio link. Data is collected at the wireless sensor node, compressed, and transmitted to the gateway directly or, if required, uses other wireless sensor nodes to forward data to the gateway. The transmitted data is then presented to the system by the gateway connection [**18, 19**].

A generic wireless sensor network is composed of a large number of sensor nodes scattered in a terrain of interest, called the sensor field. Each of them has the capability of

periodically collecting data about an ambient condition and sending data reports to a center node. Knowledge about what kind of data is concerned by a center node and propagated by that node periodically via query message. This means, each sensor can be activated; it can transmit data to its neighbors and can also communicate with the user through center node [**1, 2**]**. Figure 1** illustrates the wireless sensor network layout**.**

Sensor nodes that make up the sensor network are randomly deployed in inaccessible terrains (such as near a volcano) or disaster relief operations (such as floods and fires), which means that sensor network protocols and algorithms must possess self-organizing capabilities and exhibit cooperative higher-level behavior [**19, 20**].

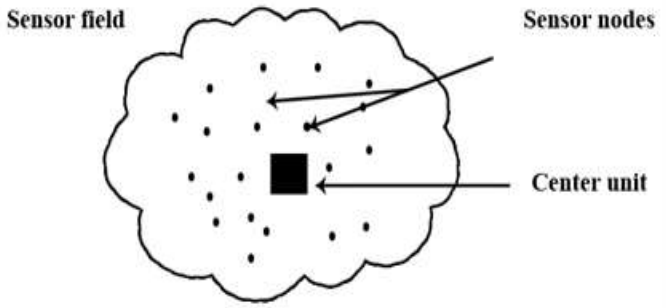


Figure 1: Sensor Nodes Scattered in the Sensor Field

D. Immune Systems

The immune system has guaranteed the health of the human body. Through identifying self and no self-mechanisms, the immune system can get rid of foreign matter (antigens) to perform this basic defense **[21, 22].**

The biological immune system (BIS) is a subject of great research interest because of its powerful information processing capabilities; in particular, understanding the distributed nature of its memory, self-tolerance and decentralized control mechanisms from an informational perspective, and building computational models believed to better solve many science and engineering problems **[3, 21].**

The biological immune system possesses capabilities of "intelligent" information processing that includes memory, ability to learn, to recognize, and to make decisions on how to treat any unknown state. The biological immune system is a highly parallel, distributed, and adaptive system. It uses learning, memory, and associative retrieval to solve recognition and classification tasks. In particular, it learns to recognize relevant patterns, remember patterns that have been seen previously, and use combinatory to construct pattern detectors efficiently. These remarkable information processing abilities of the immune system provide important aspects in the field of computation **[21,22].** This emerging field is sometimes referred to Artificial Immune System (AIS). Although it is still relatively new, AIS, having a strong relationship with other biology-inspired computing models, and computational biology, is establishing its uniqueness and effectiveness through the intensive efforts of researchers around the world **[3].**

IV. CURRENT SYSTEM DRAWBACKS AND PROBLEM DEFINITION

In existing physical access control gates, the only one information provided is the grant, which allows the object to grant entrance or deny entrance. It is important to identify, besides, the ***location***, the ***nature*** of the passing object that prohibit passing that object, and the time of passing that object the prohibited area. The passing object may be a person, a black box filled with some sort of materials, or other object with any specific characteristics. Sometimes the investigator or inspector needs more information to allow doing his job.

One situation that needs such additional information is the protection of the electricity towers distributed on desert places, in which employing guards is difficult, and surveillance cameras may cost much. In such situation we need to provide a vision for such space. If some mal material, that can make harm, exists in some location we need to define its nature and position. The above additional facts will help avoid any terrorism operations.

Accordingly, given an area ***A***, with a boundary ***B***, it is required to define the following:

- The time, ***T***, in which the mal material, or an object with a mal material has pass through the boundary ***B***.
- The nature of that mal material to detect if it is dangerous, to identify its bad effect.
- The location, ***L***, for that object in the specified area, ***A***, defined in ***x, y*** coordinates such that ***L(x, y)*** ϵ ***A*** and ***L(x, y)*** not exceeding ***B***.

It is considered that area ***A*** covers the area needed to protect the facility, equipment, or any resource inside that area.

V. THE THREE DIMENSION-BASED PHYSICAL ACCESS CONTROL GATE SYSTEM: THE PROPOSED SOLUTION

On the situation which needs the protection of the electricity towers, distributed on desert areas, a set of sensors will be distributed over such area connected together. When an object passes such area, sensors detect the nature of the material of such object. A match to the detected material with the list of materials will allow designating such material nature, and location will be detected. In this way appropriate action can be taken by security responsible.

Same idea can be applied for a variety of similar situations, which will be very helpful to apply the stated approach to secure it.

The structure of the proposed access control gate system allows, granting pass or prohibiting pass. The sensor feels the existence of a mal material in a location somewhere on the specified area, referred to, in our research as the ***location***. Such mal material is referred to, in our research as ***nature***. The time of passing through the field is the third factor in our solution, referred to as ***time***. It is important and critical since it can help in analysis of the situation. It will be much helpful if the guard knows the three facts; the ***Location***, ***nature,*** and the ***time***. This might simplify the process of investigating the passing object. This paper introduces the new idea for building the access control system that provides the three facts, which save investigation time, investigation effort, and finally

issuing appropriate and speedy decision. This, all, will be done without any human intervention.

So, already existing physical access control is a matter of whom, where, and when. Meaning, current access control system determines who is allowed to enter or exit, where they are allowed to exit or enter, and when they are allowed to enter or exit. However, today with the introduction of the electronic access means is a matter of ***location***, ***nature***, and ***time***, as previously stated.

A. The Capabilities

The proposed solution allows the detection of the nature of the mal material by distinguishing between several available mal materials. The solution can distinguish between several mal materials by learning the sensor the various types of such materials and its characteristics. A list of such materials, together with its characteristics is prepared in a database, referred to as "***mal material***" database. A match is done between the detected characteristics sensed during object passing and the list in the database. Accordingly, a decision is issued whether grant entrance or prohibit entrance. An alarm can be sent to the central system or base station, with other data, for appropriate decision. The success of such solution depends mainly on the degree of learning of the sensor with the material characteristics, and the precision of such characteristics. Examples of such sensors are Resistance Temperature, Metal detection, and Motion detection Sensors. **Figure 2** depicts this part of the proposed solution.

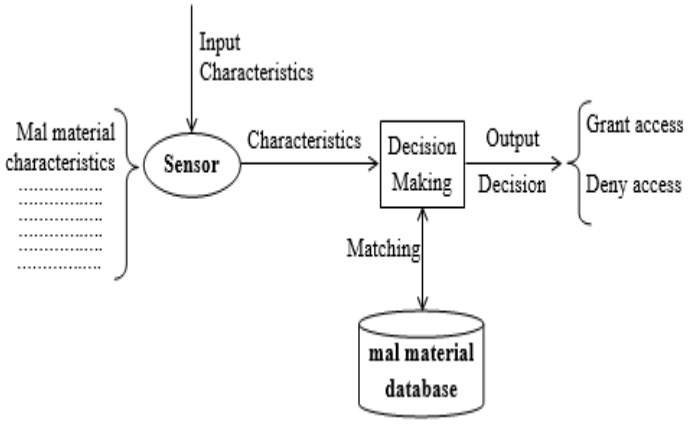


Figure 2: Detection of the Nature of the Mal Material

On the other hand, the proposed solution allows the ***location*** of the mal material to be defined by means of a sensor network that will scan the entered mal material object and detect its location. This can be achieved as follows:

- Each sensor distributed on the field has its identification code, defined location as x, y coordinates, and working status (working, or out of service).
- For the working ones, when one or more sensors senses the material object entered on the field, a message with two parameters is sent to the concentrator. The message three parameters are: the location, the nature of the material, and the time.
- The concentrator sends the central system a signal with the messages received from the all sensor network, including the three factors, the location, the nature, and the time.
- The individual sensors send the location of the object relative to their position in the field; this can lead to define the absolute location of the object in the field.
- The central system process the data received, if the nature is mal material, an alarm is sent for appropriate actions and then makes the needed analysis using the time and location.

Figure 3 depicts how the sensor network detect the location, nature, and the time and send them tom the concentrator and how the concentrator sends what he receives from various concentrators to the central system to allow precise decision making.

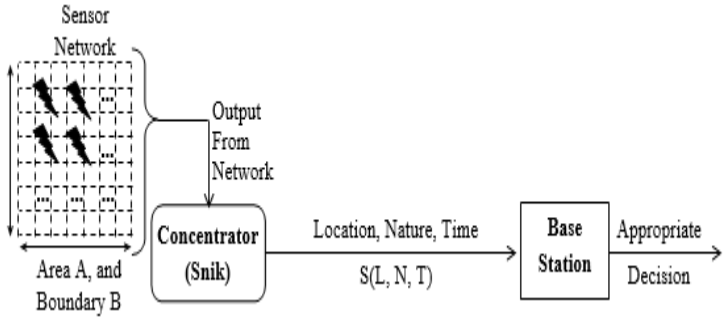


Figure 3: Location, Nature, Time Detection

B. The Architecture

First of all, the area that needs to be protected in the field is defined, in our solution; it is area ***A*** with a boundary ***B***. The sensors, then, are distributed in that area forming a wireless sensor network. Each sensor is defined to the concentrator by its code. The location of each sensor in ***A*** is detected by each one. A mapping has been defined between the individual sensor and actual field coordinates.

When an object passes the boundary ***B***, nearest sensors to that object sense such object. Each of these sensors will detect the ***nature*** of the object; define the ***time*** of detecting the object which touches the boundary, ***B***, and relative location to them. Each of these sensors will send a signal to the related concentrator with the object nature, location relative to that sensor, and the time of detection. Such sensors will continue sending such signal as much as the object is moving with a predefined rate in a second. That rate can be defined by the system operator according to degree of criticality of the protected facility. The array of signals received to the central system will be registered continually. Each current signal received will be compared to the previous signal, if changed the new signal will be the current signal. If they are equal, this means that the object has been stopped moving and the system can calculate the absolute location from the relative locations of that object to the sensors sending such signals.

The pseudo code of the proposed algorithm is as follows:

Define:

A ……..…The area is to be protected.

B ……..…. The boundary of the area is to be protected.

$L_{relative}$ ……. The location of the object related to each sensor.

$L_{absolute}$ …… The absolute location of the object to the area A.

$S_{current}$ (L, N, T) ….. The signal currently received

$S_{previous}$ (L, N, T) …. The signal previously received.

Input: Array of n-element $S_{current}(L, N, T)$;
Comment: each element consists of 3 sub elements.
while ($S_{current} \neq S_{previous}$)
continue receiving signals
endwhile
Calculate Absolute location
Detect last time received
Send $S_{current}(L, N, T)$;
exit
End

C. Designating The Object Location

The wireless sensor network is distributed over the Prohibited area A. Each sensor represents a node in this network. Each node has a specific code and the domain of each node covers a circle with a radius equal to the distance between each two sensors, as shown in the below figure. **Figure 4** shows the arrangement of the wireless sensor network and the domain of each subarea.

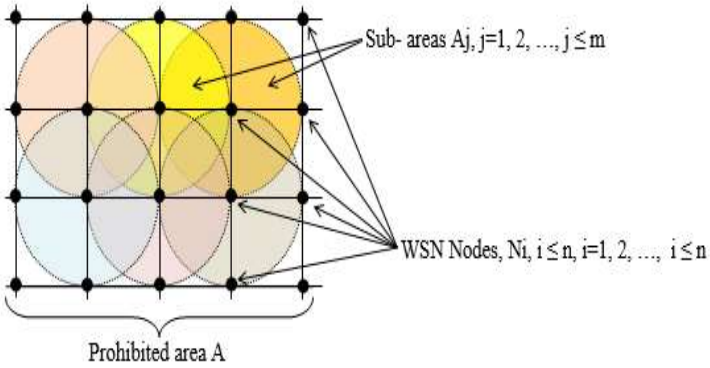


Figure 4: the Domain of Individual Sub-Areas

For the wireless sensor network covering area ***A***, given ***n*** nodes, N_i, $i \leq n$, creating ***m*** sub-areas, A_j, $j \leq m$, then:

Some sensors will sense the object passing in the prohibited area. This means that N_k , $k \leq n$ nodes will send a signal to the base station with the distance of that object to this node. The node with minimum of these distances is the node in which the object locates. Accordingly the system can designate the location of the passing object. **Figure 5** depicts an example of how to define the location of the passing object.

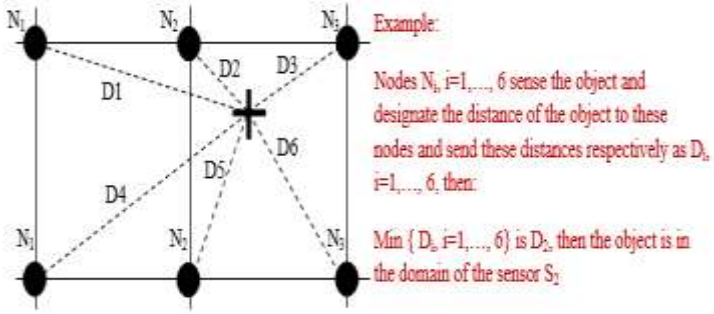


Figure 5: An example of How to Define the Location of the Passing Object.

VI. EXPERIMENTATION RESULTS

A. Experimental Configuration

As our proposed system target the application layer, there is no need for us to use a sophisticated simulation such as NS3, Cooja,.... etc. we just built our simulation using visual studio development framework (VB.Net2013) to justify that the proposed algorithm of 'Algorithm name' is sufficient using different test cases.

our simulator has a friendly GUI "graphical user interface" as shown in **Figure 6** that provides the full control of proposed system parameters such as (area, sensor range, scan period, object location, object nature). Also it provides both graphically and tabular output.

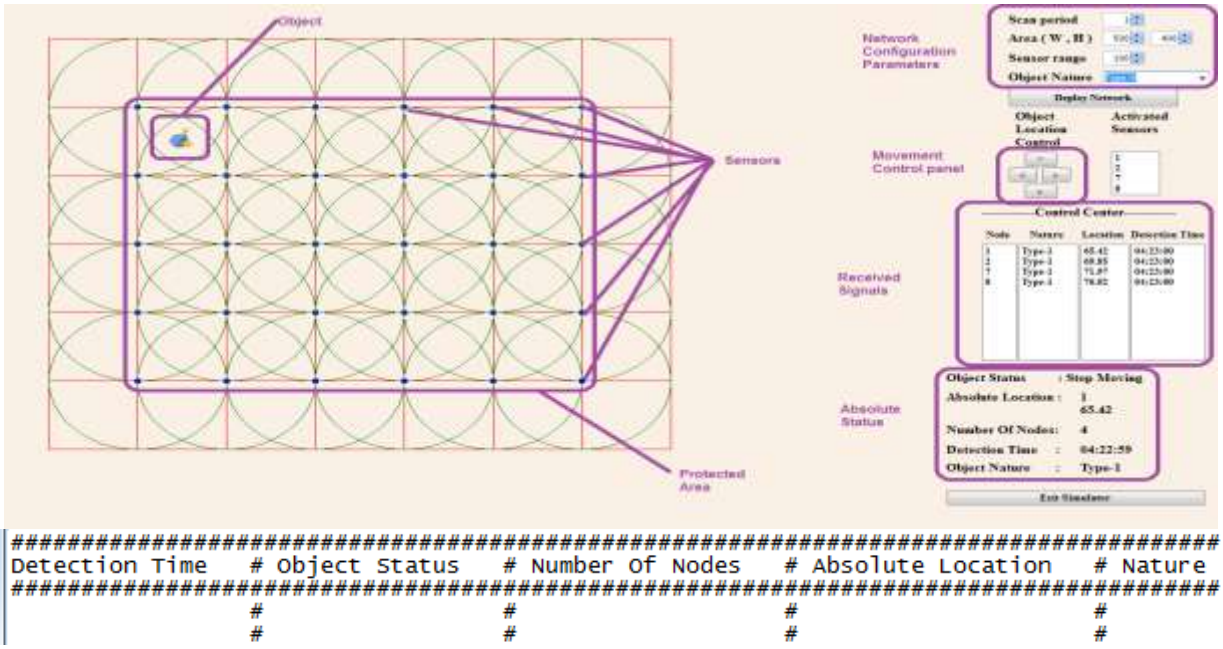


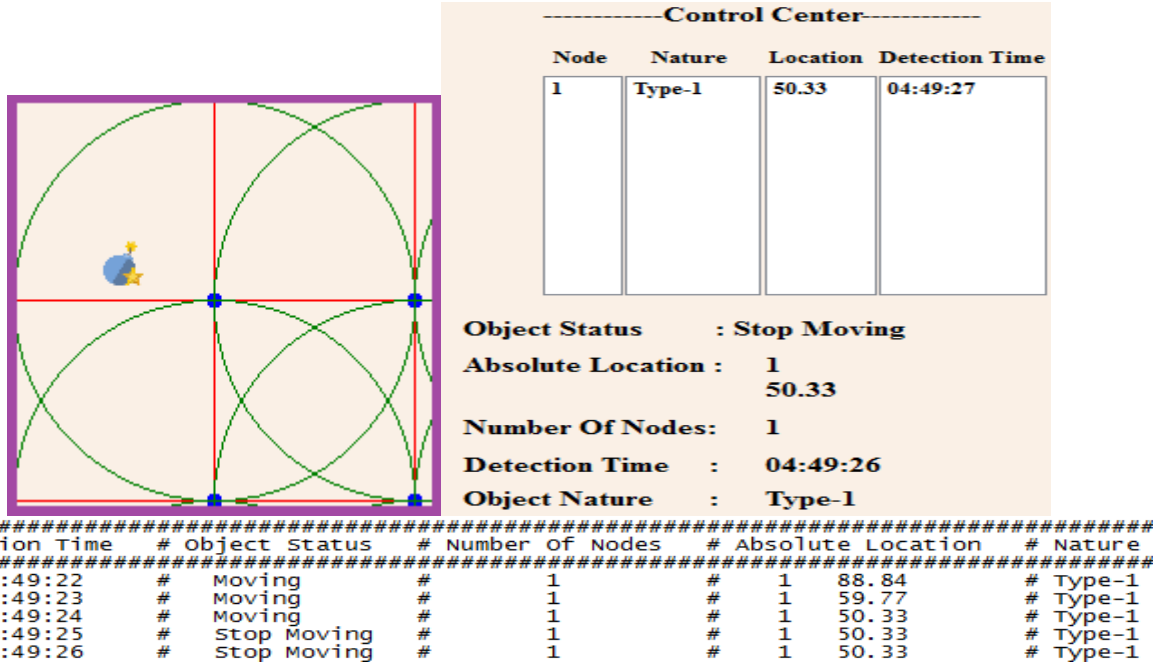
Figure 6: Graphical User Interface

We can use the real time graphical representation to monitor the moving object through the network, all received signals in the control center and the absolute status of the object (location, detection time, nature, moving status).

To simulate any of the test cases, first we need to configure our network structure using parameters of covered area (width and high), sensor range and the scan period. Then we need to configure the nature of the object material.

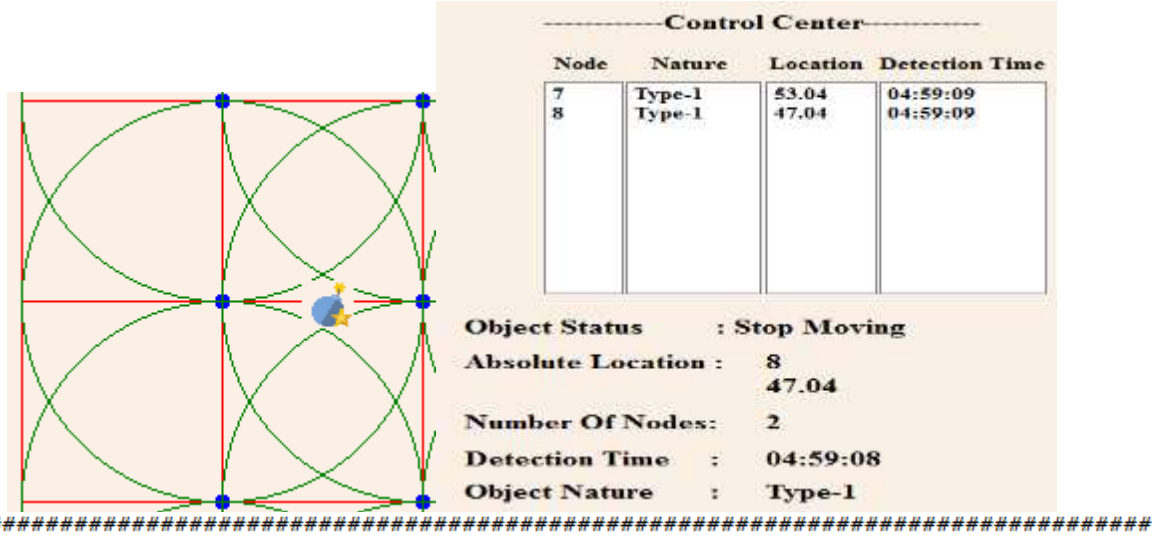
B. Obtained Results

We will apply four different test cases to ensure that the proposed algorithm is efficient. The first, second and third test case describes the behavior of a moving object passes the boundary and stop in area that's covered by the radiation of one, two four sensors respectively as shown in **Figures 7, 8, 9, and 10**. And the last test case describes the behavior of a moving object passes the boundary and moves around different areas covered by different numbers of sensors as shown in **Figure 7**.



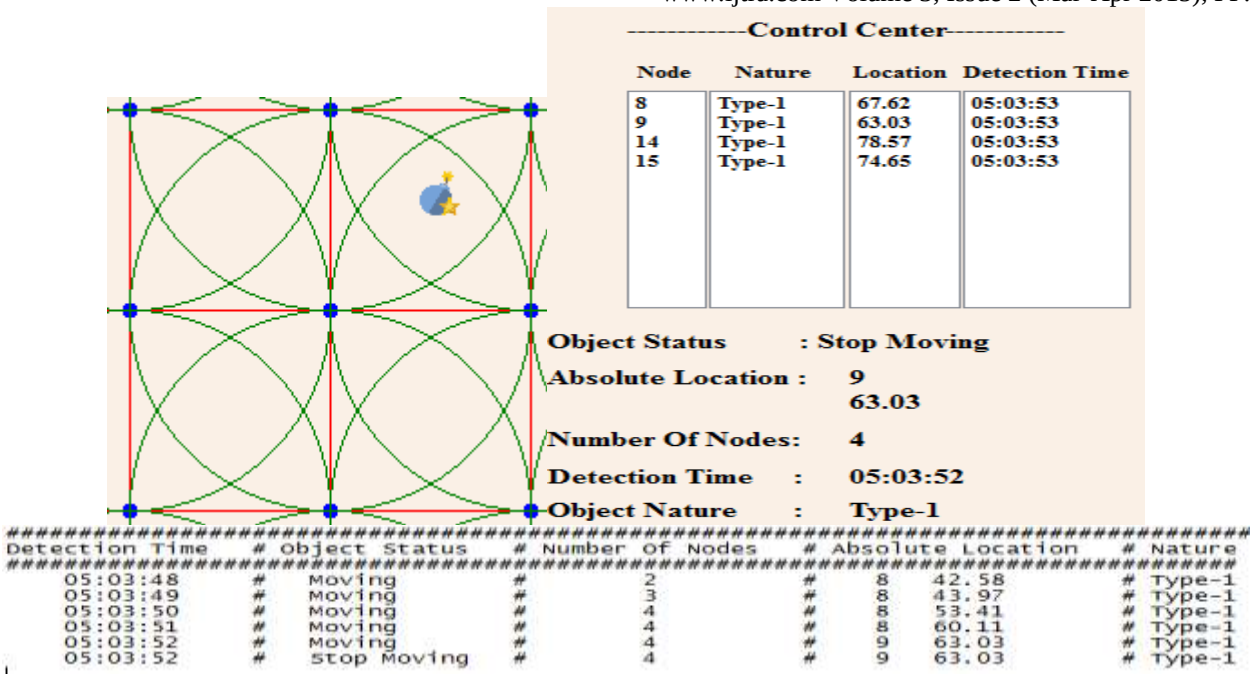
Detection Time	#	Object Status	#	Number Of Nodes	#	Absolute Location	#	Nature
04:49:22	#	Moving	#	1	#	1 88.84	#	Type-1
04:49:23	#	Moving	#	1	#	1 59.77	#	Type-1
04:49:24	#	Moving	#	1	#	1 50.33	#	Type-1
04:49:25	#	Stop Moving	#	1	#	1 50.33	#	Type-1
04:49:26	#	Stop Moving	#	1	#	1 50.33	#	Type-1

Figure 7: Test case 1 graphical and tabular output



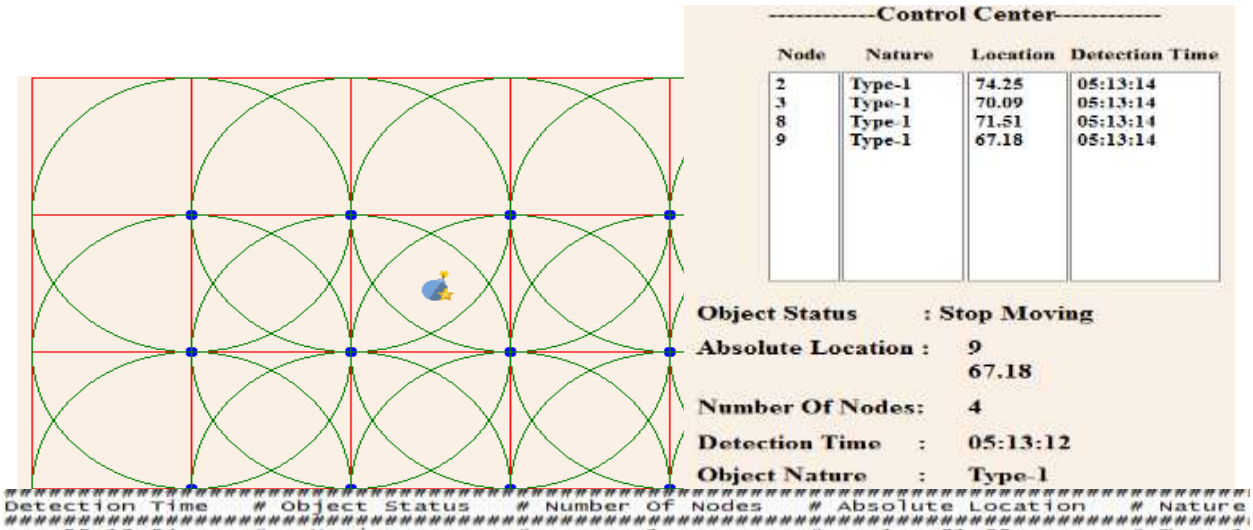
Detection Time	#	Object Status	#	Number Of Nodes	#	Absolute Location	#	Nature
04:59:05	#	Moving	#	2	#	6 78.04	#	Type-1
04:59:06	#	Moving	#	2	#	6 90.68	#	Type-1
04:59:07	#	Moving	#	2	#	8 47.04	#	Type-1
04:59:08	#	Stop Moving	#	2	#	8 47.04	#	Type-1

Figure 8: Test case 2 graphical and tabular output



Detection Time	Object Status	Number Of Nodes	Absolute Location	Nature
05:03:48	Moving	2	8 42.58	Type-1
05:03:49	Moving	3	8 43.97	Type-1
05:03:50	Moving	4	8 53.41	Type-1
05:03:51	Moving	4	8 60.11	Type-1
05:03:52	Moving	4	9 63.03	Type-1
05:03:52	Stop Moving	4	9 63.03	Type-1

Figure 9: Test case 3 graphical and tabular output



Detection Time	Object Status	Number Of Nodes	Absolute Location	Nature
05:12:54	Moving	1	1 81.93	Type-1
05:12:55	Moving	1	1 72.62	Type-1
05:12:56	Moving	1	1 54.71	Type-1
05:12:57	Moving	1	1 46.4	Type-1
05:12:58	Moving	1	1 38.9	Type-1
05:12:58	Stop Moving	1	1 38.9	Type-1
05:13:00	Moving	2	1 30.87	Type-1
05:13:01	Moving	2	1 43.28	Type-1
05:13:01	Stop Moving	2	1 43.28	Type-1
05:13:03	Moving	2	1 51.31	Type-1
05:13:04	Moving	2	2 28.86	Type-1
05:13:05	Moving	2	2 24.35	Type-1
05:13:06	Moving	3	2 12.37	Type-1
05:13:06	Stop Moving	3	2 12.37	Type-1
05:13:08	Moving	3	2 17.69	Type-1
05:13:09	Moving	3	2 35.11	Type-1
05:13:10	Moving	4	2 53.41	Type-1
05:13:11	Moving	4	8 64.44	Type-1
05:13:12	Moving	4	9 67.18	Type-1
05:13:12	Stop Moving	4	9 67.18	Type-1

Figure 10: Test case 4 graphical and tabular output

VII. THE CONCLUSIONS

In fact, the application of physical security as to pass or prohibit pass is inappropriate for specific applications. The fields and areas which are subjective to territory activities is a base example. In many places in the world, bombing can explode buildings, lives, facilities, and so many others. In such cases we need to manage the situation remotely. The paper showed that a physical access control detection system can survey the field without human direct intervention. Such system can intervene electronically to detect the parameters needed to decide the appropriate actions.

The new approach for providing the parameters needed for decision maker, in such situations, is presented, in this paper, it is the three dimension-based physical access control

detection system, with the parameters; the nature, the location, and the time. This approach depends basically on the sensor network and immune system combined with a central system that can receives a signal with such parameters to allow decision maker enough information for decision making.

REFERENCES

[1] Carlos. De morais, and Dharma. Prakash, "Ad Hoc & Sensor Networks Theory and Applications", World Scientific Publishing Co. Ptc. Ltd, 2006.

[2] K. Sohraby, D. Minoli, and T. Znati, "Wireless Sensor Networks Technology, Protocols, and Applications", Fourth Edition, John Wiley& Sons. Inc, 2007.

[3] Dipankar Dasgupta , "Advances in Artificial Immune Systems",IEEE Computational Intelligence Magazine, PP 40-49 Novembre 2006.

[4] "Chapter 1: Physical Security Challenges". Field Manual 3-19.30: Physical Security. Headquarters, United States Department of Army. 2001.

[5] Garcia, Mary Lynn (2007). Design and Evaluation of Physical Protection Systems. Butterworth-Heinemann. pp. 1–11. ISBN 9780080554280.

[6] "Chapter 2: The Systems Approach". Field Manual 3-19.30: Physical Security. Headquarters, United States Department of Army. 2001.

[7] Anderson, Ross (2001). Security Engineering. Wiley. ISBN 978-0-471-38922-4.

[8] For a detailed discussion on natural surveillance and CPTED, see Fennelly, Lawrence J. (2012). Effective Physical Security. Butterworth-Heinemann. pp. 4–6. ISBN 9780124158924.

[9] Task Committee; Structural Engineering Institute (1999). Structural Design for Physical Security. ASCE. ISBN 978-0-7844-0457-7.

[10] Baker, Paul R. (2012). "Security Construction Projects". In Baker, Paul R. & Benny, Daniel J. The Complete Guide to Physical Security. CRC Press. ISBN 9781420099638.

[11] "Chapter 4: Protective Barriers". Field Manual 3-19.30: Physical Security. Headquarters, United States Department of Army. 2001.

[12] "Chapter 6: Electronic Security Systems". Field Manual 3-19.30: Physical Security. Headquarters, United States Department of Army. 2001.

[13] Tyska, Louis A. & Fennelly, Lawrence J. (2000). Physical Security: 150 Things You Should Know. Butterworth-Heinemann. p. 3. ISBN 9780750672559.

[14] "Chapter 7: Access Control". Field Manual 3-19.30: Physical Security. Headquarters, United States Department of Army. 2001.

[15] Pearson, Robert (2011). "Chapter 1: Electronic Access Control". Electronic Security Systems: A Manager's Guide to Evaluating and Selecting System Solutions. Butterworth-Heinemann. ISBN 9780080494708.

[16] Federal Financial Institutions Examination Council (2008). "Authentication in an Internet Banking Environment".

[17] biometric access control technology overview

[18] K. Sohraby, D. Minoli, and T. Znati, "Wireless Sensor Networks Technology, Protocols, and Applications", Fourth Edition, John Wiley& Sons. Inc, 2007.

[19] M. Kuorilehto, M. Kohvakka, J. Suhonen, P. Hamalainen, M. Hannik¨ainen, and Timo D. Hamalainen,"Ultra-Low Energy Wireless Sensor Networks in Practice Theory", Realization and Deployment,John Wiley & Sons, Inc., Publication, 2007.

[20] J. S.Wilson, "Sensor Technology Handbook", Elsevier Inc. 2005.

[21] Anil Somayaji, Steven Hofmeyr, & Stephanie Forrest , "Principles of a Computer Immune System", New Security Paradigms Workshop Langdale, Cumbria UK, 1997

[22] Leandro Nunes de Castro, Fernando J. Von Zuben "The Clonal Selection Algorithm with Engineering Applications" Workshop Proceedings of GECCO'00, pp. 36-37, Workshop on Artificial Immune Systems and Their Applications, Las Vegas, USA, July 2000.