Research Article

Journal of Nuclear Technology in Applied Science
Year 2025, Volume-13

www.acspublisher.com

# Physical Security Assessments using Worst-Case Coverage in Wireless Sensor Networks

**Mahfouz, A.M.[1]; Ismail, A.S.[1]; Nasry, H.[1], Wadoud, A.A.[2,*] and Abdel-Rahman, M.A.E.[3]**

1. *Mathematics Department, Military Technical College, Cairo, Egypt.*
2. *Egyptian Atomic Energy Authority, Reactors Department, Cairo, Egypt.*
3. *Nuclear Engineering Department, Military Technical College, Cairo, Egypt.*

## ARTICLE INFO

**Keywords:** *Clifford algebra, Wireless sensor network, Worst coverage, Plane target, Physical security assess-ments, Risk model, SAVI model.*

doi: 10.48165/jntas.2025.13.1.6

## ABSTRACT

Most of the nuclear and radiological facilities have physical security systems which include different types of intrusion detection cluster sensors. They should be kept active, valid and updated and follow the requirements of the nuclear regulatory authority at the national level and meet the recommendations of IAEA at the international level. Wireless sensor networks are crucial to many applications. Nuclear facilities security systems are one of the major uses for wireless sensor networks. The majority of studies conducted on wireless sensor networks concentrate on improving target coverage to save energy consumption and network costs. One of the most important issues to take into account, when researching the coverage problem of sensor networks is the problem of planar target analysis. This study presents a new coordinate-free sensor network coverage model for the plane target issue, based on Clifford algebra which is a strong tool. Additionally, the Clifford Algebra computations of the node coverage rate for the plane target in the sensor network are illustrated. After that, the sensor network's worst-case coverage (maximum clearance path) for a plane target is provided which is used to provide security for nuclear facilities to prevent and find any intruders from making any troubles. Through simulation, the suggested algorithm's dependability and optimality have been demonstrated. Furthermore, a comparison is given between the point target's and the plane target's breach weight. In this work, a hypothetical nuclear site was assumed for both security system analysis and system effectiveness evaluation. The systematic analysis of vulnerability to intrusion (SAVI) program was used for evaluation process. SAVI determines the 10 vulnerable paths as a measure of system effectiveness. A SAVI output result shows that the effectiveness of the security system, $P_E$, along the worst vulnerability path was 82%. The System probability of detection $P_D$ was 94% of nuclear facility. This analysis concludes that the security system of HNRC facility is winning against the worst path of the terrorists attack and achieved its objective.

*Corresponding author.
E-mail address: amirwadood@gmail.com
Received: 28/06/2025 Accepted: 23/9/2025

# Introduction

Numerous applications, including robotics, military operations, environmental monitoring, target tracking, surveillance systems, and forest fire systems, are made ideal by sensor networks. Wireless sensor networks have advanced significantly as a result of their affordability and dependability. Every sensor node in the networks is capable of measuring the statuses of the targets and interacting with other nodes to exchange acquired data and perform calculations (**Jondhale *et al.,* 2022; Akkaya and Younis, 2005**). Wireless sensor networks can be classified as static networks or dynamic networks based on the node's movement capabilities. Wireless sensor towers can be classified as random deployment or deterministic deployment based on the node's deployment technique (**Temene *et al.*, 2022**). The fundamental issue with all wireless sensor networks is coverage. Three types of coverage issues can be identified with static wireless sensor networks: barrier, area, and point coverage (**Ribeiro *et al.*, 2015**). In order to characterize the network's ability to detect a target, it is necessary that the probability of a moving target not being discovered when it moves through the network deployment area along an arbitrary path be as small as possible. Therefore, for any given sensor network, it is necessary to analyze the probability of a target being detected when it moves through the network. Measuring the quality of sensor network coverage provides the concept of worst-case coverage (**Megerian *et al.,* 2005**). Exposure has been referenced in numerous sources to quantify the likelihood that a particular target will be discovered, whether or not it is detected by a sensor network. In literature (**Veltri *et al.*, 2003**), Djkastra's algorithm is used to determine the target's shortest exposure path after the target's exposure degree is computed based on the target energy gathered by the sensor network. In literature (**Yi and Chakrabarty, 2005**), two paths are calculated: the maximum clearance path and the maximum support path, exposure is defined as the distance between the standard path and the sensor node. In **Kim and Lee** (**2021**) a two-dimensional rectangular region is considered to be protected by a group of sensors, which consist of sensors or security cameras. Additionally, the minimal exposure path is determined by first utilizing the sensing ranges of the sensors to compute an estimated "feasible region" of interest, and then employing a grid to systematically search within this feasible area for the smallest exposure path. It should be noted that mobile sensors were used to examine the barrier sweep coverage (**Gorain and Mandal, 2019**), with a finite-length continuous curve on a plane serving as the model for the barrier. The function efficiency was generated by combining the calculated minimal exposed path with the ratio of covered to uncovered grids in the algorithm. The sink node used sensor node exposure measurements to determine the lowest exposure path (**Bonnah and Cai, 2019**). When determining the largest clearance path by conventional approaches, the planar target moving into the path can be mistakenly believed to be uncovered by nodes (**Nasry *et al.*, 2014**).

### *Modeling framework and research methodology*

In this study, a Clifford algebra-based coverage analysis for plane targets is proposed. Therefore, the traversal problem of two-dimensional planar targets is studied using its calculation. Consequently, it is possible to suggest utilizing Clifford geometric algebra, a tool independent of a particular coordinate system (**Breuils *et al.,* 2022**). 'By using the full relative information between sensor nodes and targets, the coverage analysis model can solve the problem of sensor network coverage. This study applies Clifford geometric algebra based on this. A sensor network maximum clearance path algorithm based on the planar target is suggested, along with the representation of the planar target and the rate of coverage for each node to the planar target. The planar target moving through the sensor network is represented by the network's Voronoi diagram (**Hao *et al.*, 2021**). Experiments demonstrate that the best path of the planar target in the sensor network, which represents the network coverage performance, can be found efficiently by applying Clifford geometric algebra. WK Clifford created Clifford algebra around the close of the 1800s. Another name for it is Exterior algebra. It was a Grassman algebra extension. Geometric symbol representations for space geometry can be computed using Clifford algebra without requiring coordinates. However, for geometric computations and analysis, it can be simply expanded to higher dimensional space (**Nasry, 2019**). It is now a crucial research tool in theoretical physics and mathematics (**Nasry *et al.*, 2014**, and**Nasry, 2019)**, and **aky *et al.*, 2023**). The inner product space  is now the most widely used algebraic structure for Euclidean n-space. This structure's effective extension is depicted in **Franchini *et al.*** (**2017)** and **Macdonald, (2010**).Additionally**,** presentation of the plane target and the computation of the nodes' coverage rate in a wireless sensor network will be introduced. Moreover, Clifford al-

gebra is used to represent the plane target and determine the maximum clearance path. Finally, Results and discussion is provided. Most of the nuclear and radiological facilities have physical security systems (PSS). The security systems include different types of cluster sensors, components and control devices. They should be kept active, valid and updated (**EI-Kafas and Wadood, 2008**), and follow the requirements of the nuclear regulatory authority at the national level and meet the recommendations of IAEA at the international level (**IAEA, Nuclear Security Series No. 13, 2011**). The physical security system (PSS), which is necessary to safeguard the nuclear site from any chance of bombing, sabotage, or theft, should satisfy the three fundamental components of detection, delay, and response (**Garcia, 2007**). The system must respond in the shortest possible time to allow enough time for the response force to arrive and defend the property a timely manner; hence thwarting the adversary and neutralizing their mission. The physical protection system's performance has to be planned to thwart and restrict the attacker's resources and strategies as they pertain to the nuclear site (**Wadoud *et al.*, 2018**).

### *Representation for plane target of sensor network*

Considering that the wireless sensor network's sensor nodes are omnidirectional and that their coverage is based on a binary perception model. Additionally, the coverage area of sensor nodes in a two-dimensional plane is a circle with radius **R**. The sensor node's "Sensing Disk" is this region, and R is its sensing range, which is established by the physical properties of the sensor node unit. When calculating the maximal clearing path (worst case coverage) in classical computer sensor networks, the target is frequently treated as a point target. As shown in Figure 1 (a), however, treating the target as a point is untrue **(Taylor, 2021; Mahfouz *et al.*, 2023)** .

As shown in Figure 1 (b), the planar target **T** on path **P** will be incorrectly calculated as not covered by a node when the conventional method of calculating the greatest clearance path is applied; nevertheless, when T is going along path P, it will be covered by nodes $S_1$ and $S_2$.

### *Plane target representation based on Clifford algebra*

This section gives an expression of the plane targets in the sensor network using Clifford algebra. The double direction of the tangent plane B can be used to represent it for a planar target (**Mann and Dorst, 2002**).

$$x \wedge B = p \wedge B \qquad (1)$$

Formula (1) is the equation of all vectors of the tangent plane B and $(\boldsymbol{p} \wedge \boldsymbol{B})$ into the point on B through p which is vertical where p is any point on the plane target. For the equation of all vectors, the support vector is $(\boldsymbol{p} \wedge \boldsymbol{B})/\boldsymbol{B}$, let $\boldsymbol{B} = \boldsymbol{b_1} \wedge \boldsymbol{b_2}$. . The vector $\boldsymbol{b}_1$ which is perpendicular to $\boldsymbol{b}_2$. So, B can be written as $\boldsymbol{B}=\boldsymbol{b}_1\boldsymbol{b}_2$.

*Clifford geometric algebra representation of the plane target in the sensor network is expressed as:*

$$x = \frac{p \wedge B}{B} + \tau_1 b_1 - \tau_2 b_2 \qquad (2)$$

*Where* $\tau_1$ *and* $\tau_2$ *are respectively,* $\tau_1 = (x \cdot b_1^{-1})$ , $\tau_2 = (x \cdot b_2^{-1})$ . The equation (2) gives the plane target parameter vector ***b1*** and ***b2***. So, ***b1*** and ***b2*** can be used. The direction establishes an affine coordinate system about the plane target.

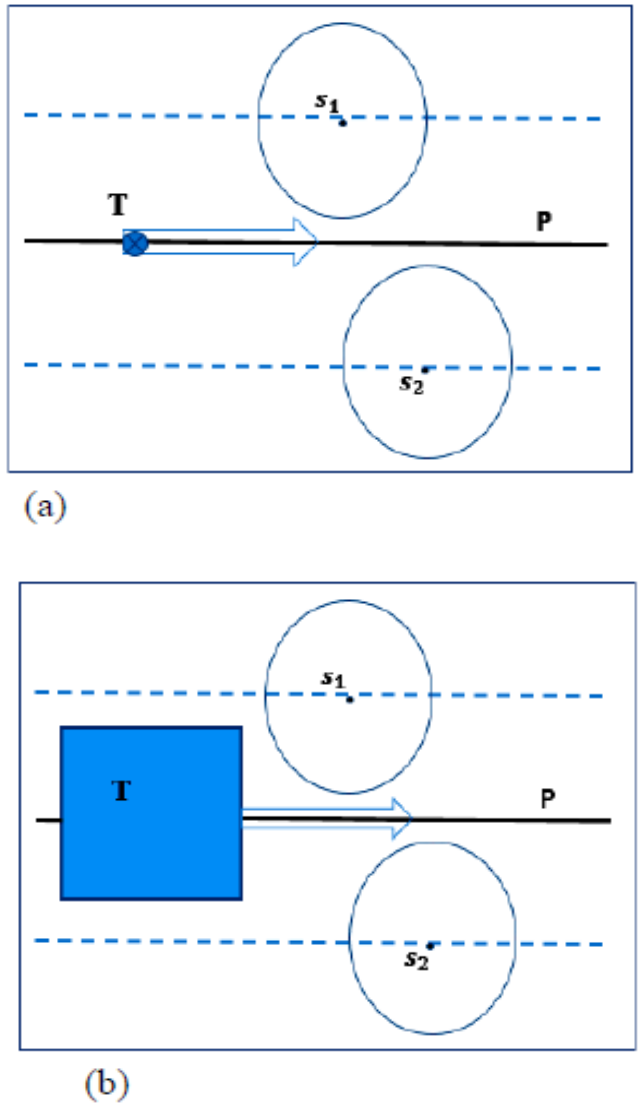



**Figure 1: (a) point target and (b) plane target through traversing path.**

***The coverage rate of nodes to plane target***

The required and sufficient requirements that indicate whether or not the sensor node S covers the target in the sensor network are given in **Xie and Meng** (**2008**). However, as Figure 2 illustrates, in practice, the plane target is entirely covered by node S if it travels across its coverage region. Determining the coverage rate of a single S node to the plane target is therefore crucial. In Figure 2, the plane target intersection with coverage area of the sensor node are represented by the parameter vectors and , let the created coordinate system's unit vectors to be and , and the nearest point to the origin is p **(Mahfouz *et al.*, 2023).**

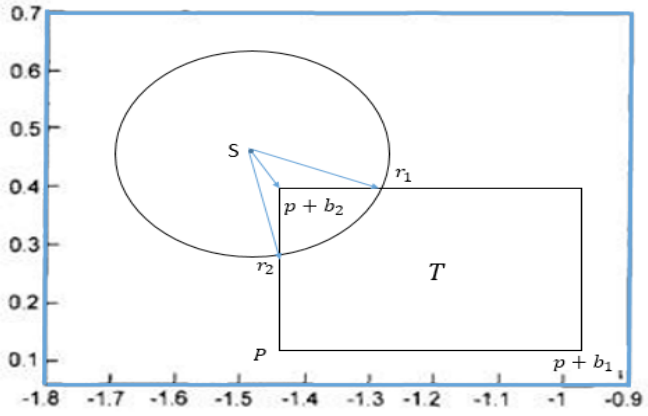



**Figure 2: Schematic representation of the intersection between single node and plane target.**

In the same coordinate system, let the node center coordinate is S, that can be expressed as, where and are the components of the node in the and directions respectively. As a result, from equation (2) and the distance relationship between points in space, equation (3) gives the coverage area of the sensor node and the plane target, where the coverage radius of the node is R.

$$x = \frac{p \wedge B}{B} + \tau_1 b_1 - \tau_2 b_2 : \|x - s\| \leq R \qquad (3)$$

Here $\| \ \|$ represents the modulus of the vector. The four endpoints of the target can be expressed as $\boldsymbol{p}$, $\boldsymbol{p}+\boldsymbol{b_1}$, $\boldsymbol{p}+\boldsymbol{b_2}$ and $\boldsymbol{p}+\boldsymbol{b_1}+\boldsymbol{b_2}$,where the vector $\boldsymbol{b_1}$ and $\boldsymbol{b_2}$ is vertical. As a result, if the node coverage area intersects the plane target, it must intersect or be tangent to the edge of the plane target as shown in figure 2. Set the intersection nodes as $\boldsymbol{r_1}$ and $\boldsymbol{r_2}$ respectively, then let the vector $\boldsymbol{k_1}=\boldsymbol{r_1}-\boldsymbol{S}$ and the vector $\boldsymbol{k_2}=\boldsymbol{r_2}-\boldsymbol{S}$. Obviously, $\|k_1\|=\|k_2\|=\mathrm{R}$.

Suppose the angle between $\boldsymbol{k_1}$ and $\boldsymbol{k_2}$ is θ, then the area of the sector $r_1r_2 = \frac{\theta}{2\pi}\pi R^2 = \frac{\theta R^2}{2}$ , where the angle θ is a vector angle. In (17) it is found that $= \tan^{-1}\frac{k_1 \wedge k_2}{k_1 . k_2}$. Let $a = p + b_2$, then the area of the triangle $\boldsymbol{Sar_1}$ is $A_{Sar_1} = \frac{\|a - s\| R sin\alpha}{2}$ where, $\alpha = \tan^{-1}\frac{k_1 \wedge (a-s)}{k_1 . (a-s)}$ . The same $A_{Sar_2} = \frac{\|a - s\| R sin\beta}{2}$ where, $\alpha = \tan^{-1}\frac{(a-s) \wedge k2}{(a-s) . k2}$, and the area of the plane target is $A_T = \|B\| = \|b_1 b_2\|$. So the coverage rate of the node to the plane target at this time $r = \frac{A_S}{A_T} = \frac{\frac{\theta R^2}{2} - (A_{Sar_1} + A_{Sar_2})}{\|B\|}$.

***Maximum clearance path for planar target***

A path that reduces the distance between each site on the path and the sensors is known as the maximum clearance path. It runs from a source to a destination. A network intruder will try to cross the sensor field and avoid the sensors as much as possible in order to avoid being discovered. The maximal clearance path in this case is the detector's worst path. The Voronoi diagram can be used to find the maximal breach path, according to Meguerdichia **(Meguerdichian *et al.*, 2001; Gau and Peng, 2006; Megerian *et al.*, 2005** and **Chang *et al.*, 2010**) furthermore investigated the deployment issue to improve the maximal breach path.

To determine the clearing path for a sensor network, the following formalization of the problem will be used: Given: A wireless sensor network with known locations for every sensor that was previously installed using deterministic or random deployment.

**Definition for Breach weight**: The lowest Euclidean distance between a path P and any sensor in the network, given the path P connecting locations I and F.

**Problem:** Determining the network's maximum clearance path that connects locations **I** and **F**. **Note:** Instead of being viewed as a point target, the target that crosses the network via the discovered path is a plane target. The idea of the plane target's coverage rate can be used to choose the path with the biggest gap based on the coverage rate. A schematic diagram of the path's sensor network nodes' coverage is displayed in Figure 3. The two dotted lines show the area that the planar target must go across, while the solid line shows the target's travel path. Based on formula (4), it is evident from Figure 3 that the node's coverage area on the intended travel path. By expressing formula (4) in integral form, it is possible to calculate the area that each node covers. This coverage area can be represented as follows:

$$A = \int_{\|x-s\| \leq R} \left(\left(\frac{P \wedge B}{B}\right) + \tau_1 b_1 - \tau_2 b_2\right) dx \qquad (4)$$

As a result, the coverage weight of the sensor network nodes for the plane target on path will be computed by equation (5):

$$w = \frac{A}{A_T} = \frac{\int_{\|x-s\| \leq R} \left(\left(\frac{P \wedge B}{B}\right) + \tau_1 b_1 - \tau_2 b_2\right) dx}{\|B\|} \qquad (5)$$

There must be at least one Maximal Clearance Path present in each line segment of the Voronoi diagram created by the sensor locations in S. The resulting Voronoi diagram shows that the closest sites' distance is maximized. Any location p on the path P that deviates from Voronoi line segments will, by definition, be at least one sensor in S closer **(Mahfouz *et al.*, 2023).**

***Presented Algorithm***

The search algorithm of the greatest gap path **P** is as follows in order to locate the maximum breach path p in the network: Each node position in the sensor network S has a Voronoi diagram **D** that is established in many spaces. Determine the weight allocated to each edge of the Voronoi diagram D in order to create an undirected weighted graph **G**. This can be done by calculating the coverage weight of each node to the plane target on each edge based on the parameter vector of the plane target. Determine the greatest gap path P from the weight of each edge by applying the binary search method and breadth-first search. The target employed in the algorithm that is being given is a plan target rather than a point target, which sets it apart from other algorithms. This will improve the network's coverage since, in the case of a point target; the path that was acquired indicates that the target is not covered, even though at least one sensor node may be able to detect it. Therefore, it is impossible to ignore the target's dimensions. Table 1 shows the presented algorithm **(Mahfouz *et al.*, 2023).**

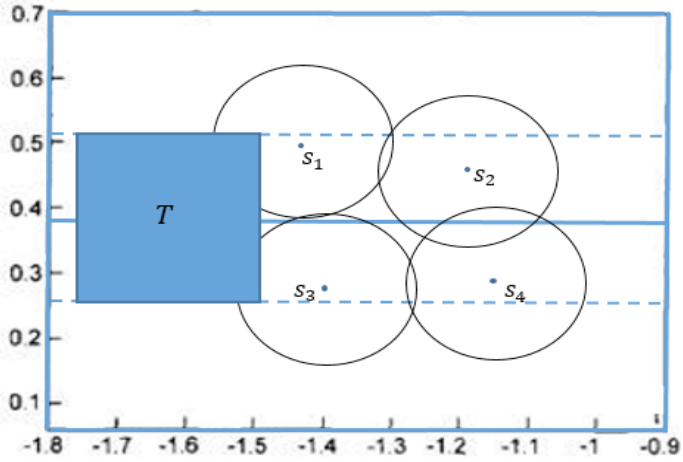



**Figure 3: Plane target passing sensor network.**

**Table 1: Presented Algorithm: Finding Breach Weight**

Generate bounded Voronoi diagram for S with vertex set U and line segment set L
Initialize weighted undirected graph G (V, E)
**FOR each vertex** $u_i \in$ **U**
    **Create duplicate vertex** $v_i$ **in V**
**FOR each** $l_i$ $(u_j, u_k) \in$ **L**
    **Create edge** $e_i$ $(v_j, v_k)$ **in E**
Weight $(e_i)$ = min distance from sensor $s_i \in$ S for $1 \leq i \leq S$
min_weight = min edge weight in G
max_weight = max edge weight in G
range = (**max_weight** - min_weight) / 2
breach_weight = min_weight + range – plan_target
**WHILE** (range > binary_search_tolerance)
Initialize graph $G'(V', E')$
**FOR each** $v_i \in$ **V**
    **Create vertex** $v_i$ **in** $G'$
**FOR** each $e_i \in$ **E**
    **IF** Weight $(e_i) \geq$ breach_weight
        **Insert edge** $e_i$ **in** $G'$
    **IF BFS (**$G'$**, I, F) is successful**
breach_weight = breach_weight + range– plane_target
**ELSE** breach_weight = breach_weight + range
**END IF**

***Physical security system effectiveness evaluation***

To make sure a PPS achieves its goals, it needs to be examined and assessed after it is designed. The product of two probability determines the physical protection system effectiveness (PE) along a given path (**Oyeyinka *et al.*, 2014**)

$$P_E = P_I \times P_N \quad (6)$$

Where: $P_I$ stands for the probability of interrupting the attack, which is the chance that the response force will arrive at the target promptly enough to prevent the opponent from moving forward. $P_N$ is defined as the likelihood of neutralizing the adversary, where the probability that the response force will be physically stronger than the adversary to capture or liquidate them or cause the adversary to flee. Also, in the case of just one sensor along the path, the probability of interruption is computed as the following:

$$P_I = PD \times PC \quad (7)$$

Where: $P_C$ represents the likelihood of guard communication and $P_D$ denotes the likelihood of detection. When there are several detection sensors in an adversary's path, the following equation represents the $P_I$ value:

$$PI = P(D_1) \times P(C_1) \times P(R|A_1) + \sum_{i=2}^{n} P(D_i) \times P(C_i) \times P(R|A_i) \times \prod_{i=1}^{i-1} (1 - P(D_i)) \quad (8)$$

**(Wadoud, *et al.*, 2019)**

Where: P (Di) represents the likelihood of an alarm for the facility's equipment, such as infrared (IR) sensors, being detected. P (Ci) is the likelihood that the facility guard will successfully use the tools available to them to comprehend the alarm state and will then successfully relay that information to the response force. P(R/A) is the Probability of response force arrival ($A_i$) prior to the end of the adversary's action sequence given an alarm.

$$P(R/A) = \int_0^{\infty} \frac{1}{\sqrt{2\pi\sigma_x^2}} \exp\left[-\frac{(x-\mu_x)^2}{2\sigma_x^2}\right] dx \quad (9)$$

The probability of interruption $P_I$, it is calculated by different evaluation methods as:

- **E**stimate of **A**dversary **S**equence **I**nterruption **(EASI)** Program **(Norichika, 2014)** , (Single path Pc program),
- **S**ystematic **A**nalysis of **V**ulnerability to **I**ntrusion **(SAVI)** Program (**Matter, 1988),** (Multi-path Pc program)

In this work, SAVI Program will be used for determining $P_I$

***One Dimensional (1-D) Risk Model***

As aforementioned, effective security system designs must begin with a clear definition of the target that needs to be of the repercussions involved. One form of a risk equation is given by **Rother *et al.* (2016; Wadoud, (2019**).

$$R = P_{AA} \times [1 - (P_I \times P_N)] \times C \quad (10)$$

Where, **R:**the remaining risk level. $P_{AA:}$ the probability of an adversary attack

**C:** the consequence & it has range from 0 to 1. it determined by regulatory body

Due to a lack of information and the inability to "read the minds" of potential adversaries in advance, it is exceedingly difficult to assess the likelihood of an adversary attack. Consequently, it is customary to assume $P_{AA}$= 1.0 (certainty of attack), in which case conditional risk is commonly used to describe the outcome. The conditional risk ($R_C$) can be computed by the equations:

$$R_C = [1 - (P_I \times P_N)] \times C \quad (11)$$

## Results and Discussions

Figure (4) illustrates the clearance path for a plane target through a 10 random distributed sensor network. The algorithm to find the maximum breach path is used to construct the breach path of a plane target crossing the sensor network, which is represented by a randomly configured set of 10 nodes deployed in a specific region. A comparison of the maximum breach weights of point targets and flat targets across varying node counts is presented in Figure 5. The maximal breach route in the event of a plane target is obviously the largest.

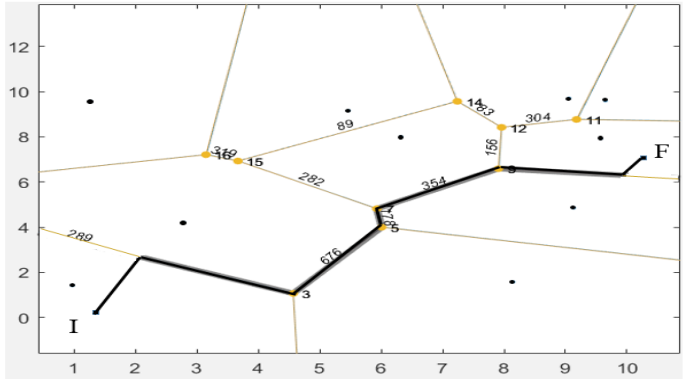



**Figure 4: Maximum breach path for a plane target.**

Figure (5) illustrates how the number of nodes in the sensor network improves coverage quality because an increase in nodes also results in a drop in breach weight. This enhances the target's ability to be monitored. Thus, there is a decreased chance that the target will go undetected. When the number of sensor nodes is same, the plane target's breach weight is higher than the point target's breach weight. This is due to the fact that both the plane target's

area and the sensor node's coverage area are taken into account when determining the maximum breach weight for the target.

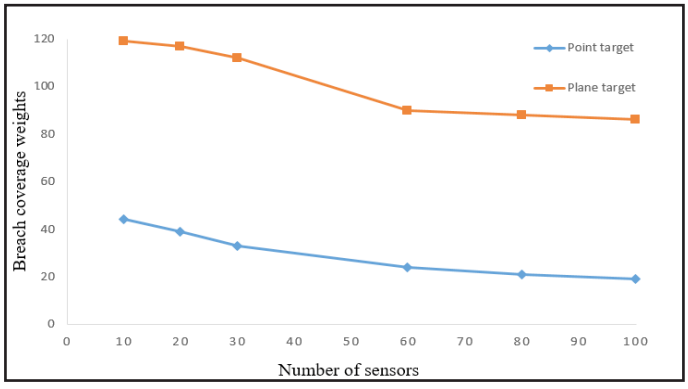



**Figure 5: Comparison between point and plane targets clearance path weights while crossing sensor network.**

The average increase for breach weight coverage by adding up to four more sensors to the network is shown in Figure (6). It should be noted that the procedure was repeated to determine the new breach weight for every placed sensor that was successful. The average improvement across 100 randomly placed sensors is displayed. It is evident that adding just one extra sensor results in a roughly 10% increase in coverage **(Mahfouz *et al.*, 2023).**

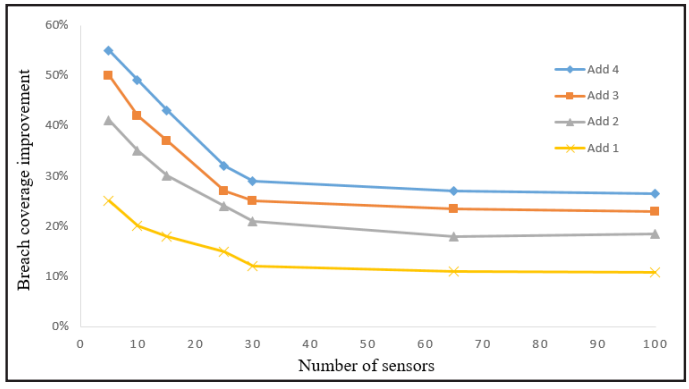



**Figure 6: Breach coverage improvement by applying four additional sensors.**

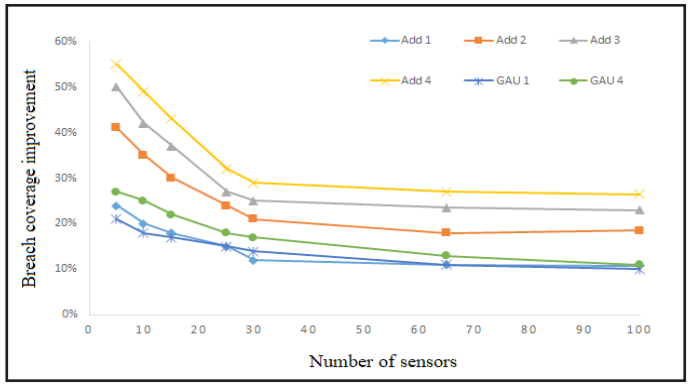



**Figure 7: Breach coverage improvement compared with GAU (Gau and Peng, 2006).**

***Advantages of this algorithm***

1. The worst-case path results are discovered, which will affect the network node deployment to improve the network's overall coverage.
2. t can be applied for sensor network path planning, target tracking and several applications.

Sensor network coverage is enhanced.

***Disadvantages of this algorithm***

1. The locations of the sensor nodes must be known in previously
2. Possible obstacles that may face the target, environment and noise are not considered.

Based on the parameter influence experiment, we concentrate on how well the three algorithms perform when the more important parameter, the number of sensors n, is changed. As network scale increases, the three methods' performance on increasing breach value diminishes, as shown in Figure 8 for the four values on the count of additional nodes. Our plane target technique outperforms the MBP-CSN and MST algorithms in some scenarios with respect to breach improvement ratio. The advantage of using the plan target algorithm is clear when four additional sensors are added, as this is when the performance difference between them is largest **(Mahfouz *et al.*, 2023).**

***Physical security system evaluation***

Moreover, this paper introduces a Hypothetical Nuclear Research Complex (HNRC) for physical security system (PSS) effectiveness analysis and evaluation process. SAVI is a computer program employed to assess this effectiveness (efficacy), and determines the most vulnerabilities and threat of PSS entry path elements on HNRC.

***HNRC-site description& intrusion detection sensors***

A hypothetical nuclear site serves as a simulation site for the physical security system's (PSS) design process. To make sure a PSS achieves its goals, it has to be examined and assessed once it is developed. The following structures and sectors may be found in the research reactor facility (RRF) location, which is located in a fictitious country, the site consists of: main entrance, security check point, research reactor (build A), and nuclear fuel plant (build B), Waste storage facility (build D) and Electrical substation (buid C). An exterior double peripheral fence, which is regarded as the first perimeter fence, must encircle the nuclear complex area. HNRC site has Underground Cable

Corridor (Electric Duct ($DUCT_1$)), crossed the external perimeter fence to ensure back-up of electric power to the HNRC, a cable corridor was created 3 meters underground leading from a nearby substation to the HNRC's electrical substation. Cable corridor cross-section dimensions are 1.4×2.1 meters. $DUCT_1$ does not boast further security protection. It is hence considered vulnerability - intruders may try to enter the electric cable corridor and crosses the fence area and path towards the protected area. The HNRC site includes a single main entrance and two gates: the vehicle gate and the personal portal gate, both of which are situated in the center of the left side of the fences. After passing the gates, there is a protected area. Figure 9 shows the site general view without any installing of physical protection sub-systems.

The **HNRC** site includes the reactor building and is composed of 3 internal floors. A top view of the floor is extracted from the architecture structure drawings. The reactor hall has the main open pool top edge and the nuclear materials (Fuel Plates) has been located inside.

The reactor is protected by internal alarm system consists of clusters of intrusion detection sensors like: Passive Infrared (**PIR**), Glass Breakage (**G.B**), and Magnetic Open Door contact (**O.D**)

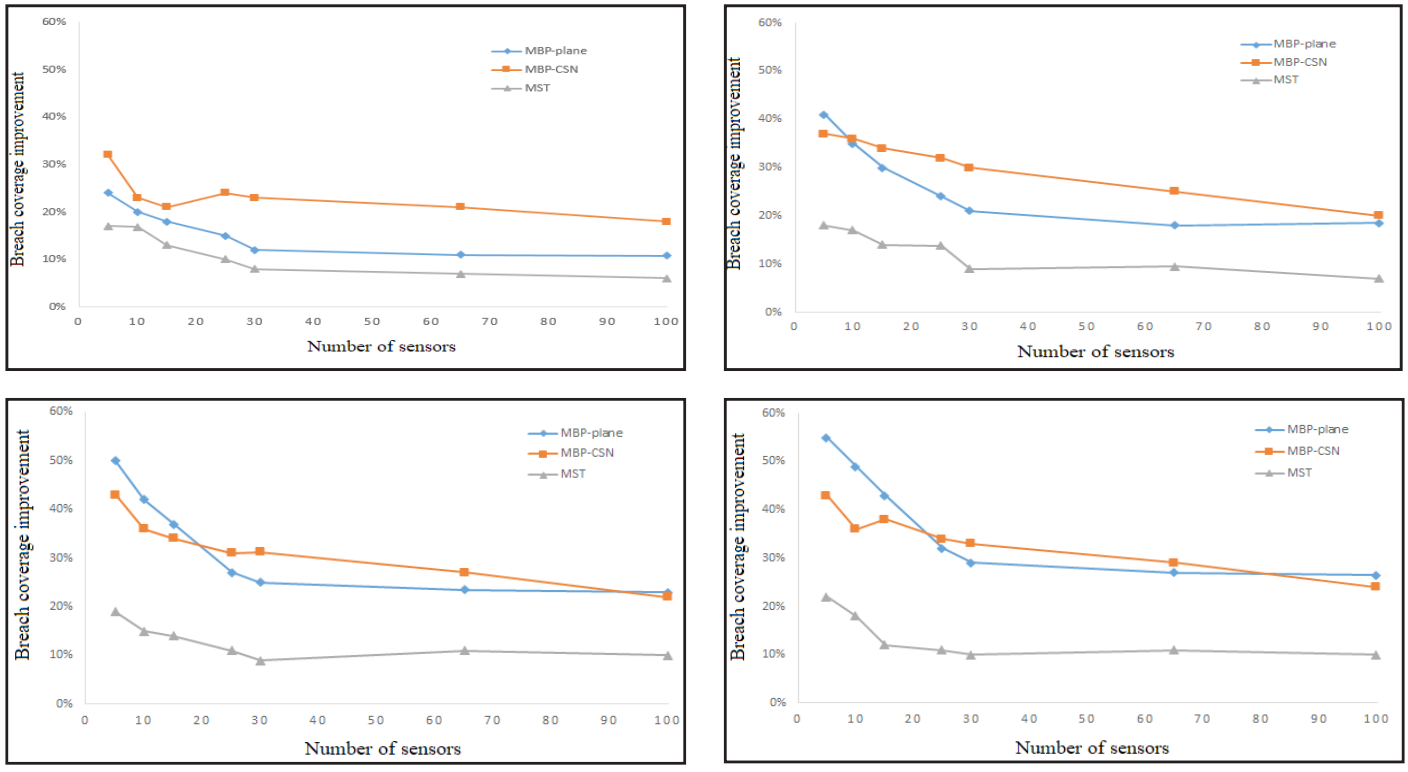



**Figure 8: Breach coverage improvement (a) while deploying one additional sensor, (b) deploying two additional sensors, (c) deploying three additional sensors and (d) deploying four additional sensors. Compared with MBP-CSN (Hong et al., 2017) and MST (Lee, et al., 2013).**

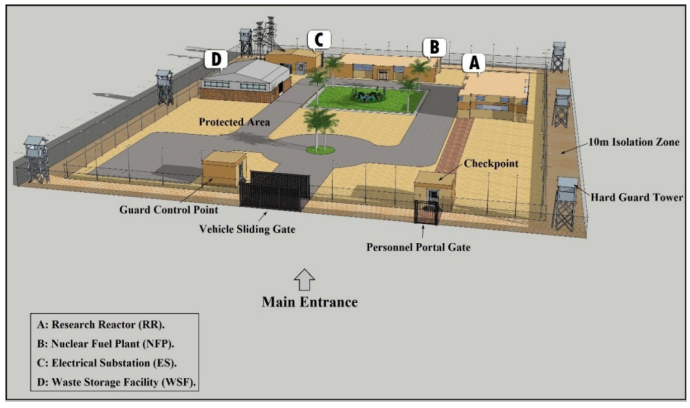



**Figure 9: HNRC facility-site view schematic drawing, without installing PPSs.**

### *Passive infrared sensors (PIR)*

Motion-activated passive infrared sensors are passive devices that can identify changes in the thermal energy pattern brought on by a moving intruder and sound an alert when they see changes in the energy levels in the surrounding area. The infrared energy spectrum has wavelengths ranging from 1 to 1,000 microns, and any object with a temperature higher than zero emits thermal energy. Since the human body emits heat energy at wavelengths between 7 and 14 microns, PIR motion sensors are usually made to function in the far-infrared region, which spans 4 to 20 microns see sensor field of view in fig 10 **(Wadoud, 2017)**.

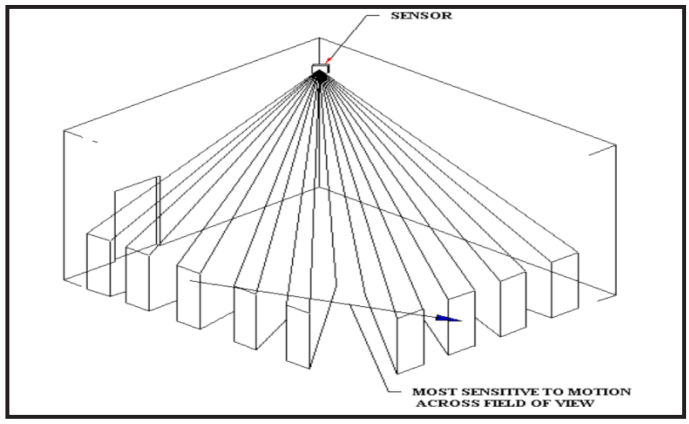



**Figure 10: Dimensions of the PIR field view.**

### *Glass-breakage sensors (G.B)*

A glass break sensor is, as its name implies, any device designed to identify the shattering of glass that is protected. Both audible and ultrasonic frequencies (20 Hz–20 kHz) are present in the noise produced by cracking glass. Glass breakage sensors detect glass breaking using microphone transducers. The configuration of G.B detector using this device is shown in Figure 11.

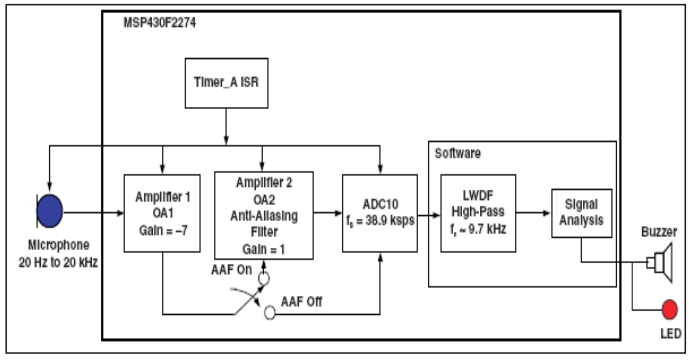



**Figure 11: Configuring the glass break detector.**

### *Balanced magnetic switches (BMS)*

A door's opening, and windows, hatches, gates, and other structural elements that may be opened to allow entrance is usually detected by BMS. Mount the actuating magnet on the door and the switch mechanism on the door frame when utilizing a BMS. A three-position reed switch and a second magnet, known as the bias magnet, are usually found next to the switch in a BMS. Interacting magnetic fields hold the reed switch in the balanced or center position when the door is closed. The switch becomes imbalanced and sounds an alert if the door is opened or if an external magnet is placed close to the sensor in an effort to disable it. When a door or window is opened, a BMS has to be installed such that the magnet experiences the greatest amount of movement. Figure (12) shows balanced magnetic switch positions (BMSs).

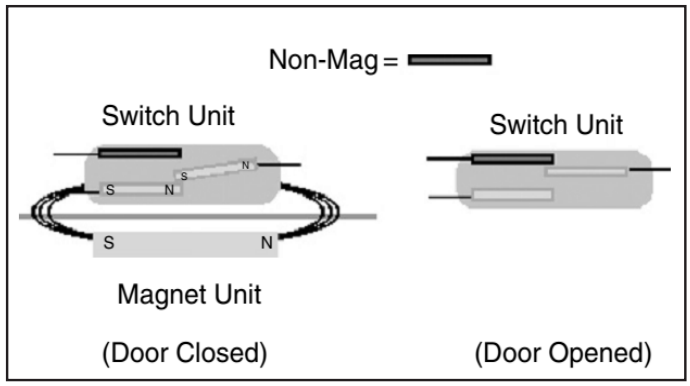



**Figure 12: Balanced magnetic switch position.**

Figure 13 shows the optimal cluster sensors distribution inside the inner area at RR and its optimal numbers: 23 PIR, 11 GB, and 30 OD, this distribution depends on the working field of view or coverage distances for each type of the cluster sensors. PIR sensor is covers 8 meters radius distance around the sensor location. G.B covers 6 meters far distance from the glass windows. BMS sensors numbers depends on the RR door numbers.

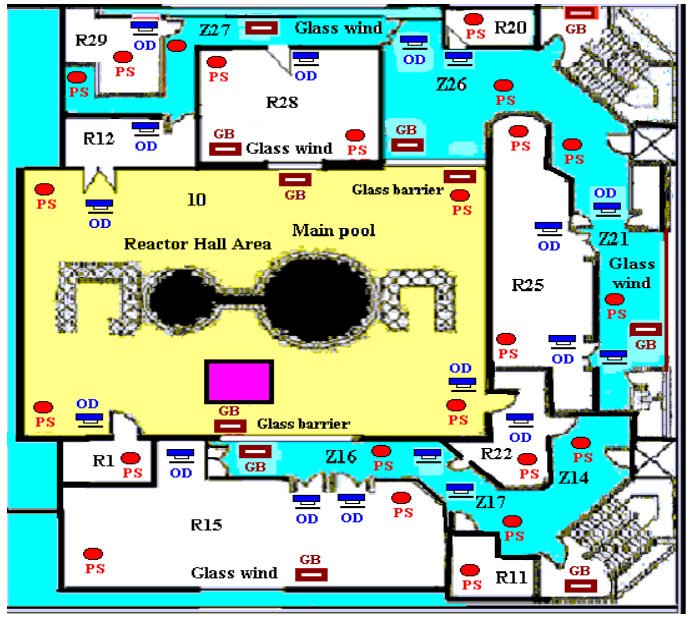



**Figure 13: Balanced magnetic switch position.**

### *Evaluation Process using SAVI Module*

SAVI has been employed to assess the PSS's efficacy and performance. As a measure of efficacy, SAVI identifies the **10 worst pathways** (the most vulnerable paths) in an adversary sequence diagram. The first steps in a SAVI analysis are target identification and target-specific adversary sequence diagram (ASD) construction. The threat's attributes must then be described. Delays, detection values, and response force deployment times must also be specified for every ASD protective element. The SAVI module

receives this data as input. The adversary sequence diagram's module determines the likelihood of an interruption for every path **(Matter, 1988)**. SAVI features include a library of safeguards components with a detection/delay performance database, a graphic representation of the findings, and recommendations for path upgrades in addition to analysis of all adversary paths. As a result, this technique makes it feasible to examine each path that an assault may take and determine which ones are the most vulnerable, as well as where crucial detection points would be located on each path. It makes use of a multi-path model of ASD, in which the pathways that connect the facilities are depicted **(Wadoud, 2018**, **Matter, 1988, and Garcia, 2005)**). SAVI software is divided the facility into two input and output modules:

- The input module makes the facility to be modelled using protective elements
- The Outsider module makes it possible to calculate the chance of an attack interruption and determines which pathways are the most vulnerable **(Matter, 1988)**.

### *HNRC PPS Evaluation (SAVI Outsider Module Results)*

Using the SAVI facility module for doing the HNRC-Site modeling, facility setting, and adversary characterize, and response forces data input information, we choose the number of paths and run the analysis from the control panel. After the analysis is finished, the outsider module analysis result shows the most vulnerable path through the PSS in the HNRC. Figure 14 shows the sabotage scenario of the adversary for the most vulnerable path to achieve his tasks Adversary is entering the limited access area from the offsite via the perimeter fence area through Underground Cable Corridor (Electric duct) and run fast towards the reactor building RR through the protected area.

Adversary continue and entering the limited access area from the offsite via the perimeter fence area through Underground Cable Corridor (Electric duct) and run fast towards the reactor building RR through the protected area. The terrorist enters RR building through the facility ventilation duct leading to the reactor building (Ground level) then take an elevator (SHP) from RR level #1 which can access RR level #3, then to the reactor area through the glass window at the reactor hall border and finally to the reactor pool which serves as the sabotage target. Any path may be chosen using the control panel. Any editor information can be achieved, and the output graphs (sensitivity, distribution and vulnerability) can be shown. Within the results box, there is a comprehensive textual description of the path that includes specific safeguard performance values and ways of incursion. A graph showing the sensitivity of the protection system to response force deployment time is one of the user-selectable features about the sets of pathways that are displayed in the graphs window**.**

Figure 14 shows the most vulnerable path which is path #1.

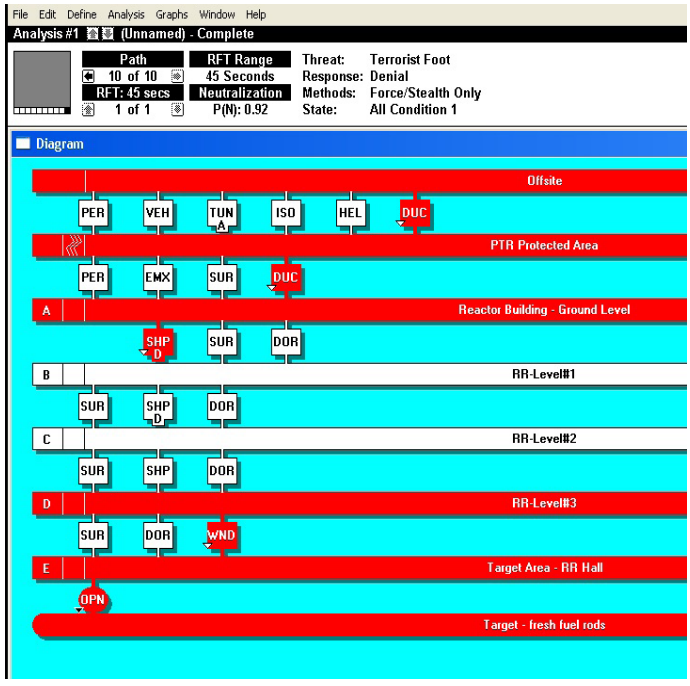



**Figure 14: The most vulnerable path of the adversary sabotage scenario.**

### *PPS Evaluation Results*

After run the SAVI outsider module; the analysis result determined the most vulnerable path and the the probability of interruption ($P_I$), the probability of neutralization ($P_N$) and the system win probability ($P_W$), the following results were obtained and illustrated in Figure 15.

Where: Detection points: are the points that the adversary supposed to be interrupted at these points through the ten vulnerable paths, and the effectiveness of the physical protection system 0.8257 which is the system potential that adversaries can be detected and assessed in sufficient time for security forces to intervene and neutralize them before they can seize or sabotage nuclear material **(Abo-Bakr, 2019**; **Elsamahy, 2021) .** The SAVI evaluation of the current PPS showed that $P_I$ is 89% and although $P_N$ is quite high 0.92, and the system win propability $P_W$=82%. Figure 16 shows The SAVI output graph which explains the relation between PI and the time remaining after interruption (TRI).

**SAVI OUTSIDER MODULE RESULTS**

Most Vulnerable Path#1 adversary sabotage scenario

P(I) Interruption Probability: 0.8975

P(N) Neutralization Probability: 0.9200

P(W) System Win Probability: 0.8257

Detection Potential (points): 22

DRFT Deployment Response forces Time #1 (Seconds) =45

TRI-Time Remaining after interruption (Seconds): 130

CDP- Critical Detection Points at open Location- fuel Rods in racks on Entry

Location in: Target Area-RR Hall

Cumulative Path Delay after CDP (Seconds): 144

**Figure 15: SAVI Outsider module PSS evaluation result.**

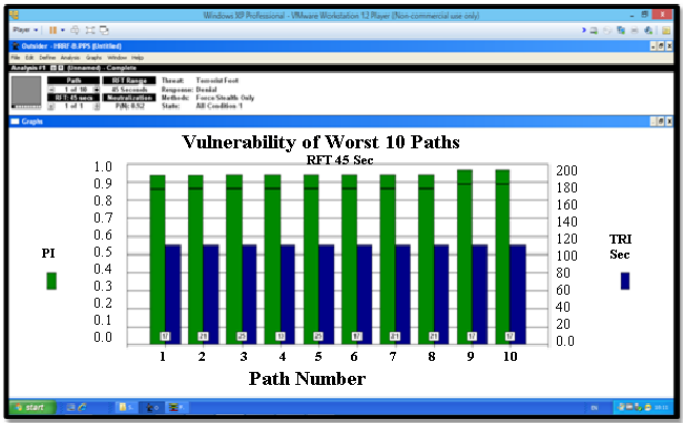


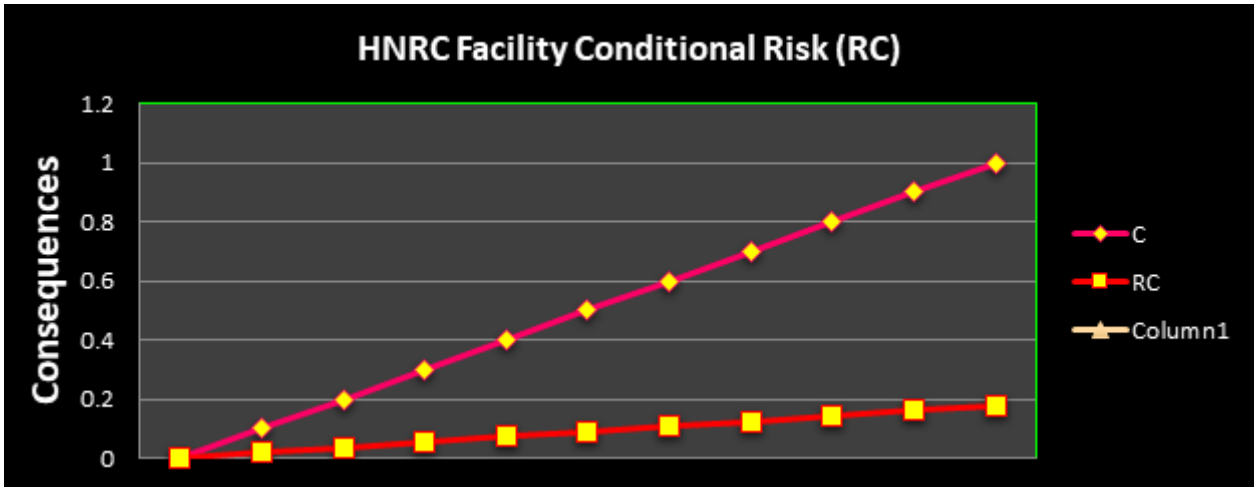

**Figure 16: The most vulnerable path of the adversary sabotage scenario.**

From the obtained SAVI results it is noticed that, The probability of interruption (PI) was 89% and the terrorist's time delay (TD =13.45 minutes) in completing his mission. The terrorist path critical point was point #10 at the ventillation Duct; this is the last point along the PPS system detection path with probability of detection, PD=94%, and the need deployment response time is 45 seconds at the site and the response forces still have a time of 5 minutes to stop the terrorist and 130 seconds remaining after the neutralization of the adversary. Final the security system of HNRC facility is win against the worst path of the terrorists attack and achieved its objective.

### *Conditional risk ($R_C$) and consequences (C) calculations*

Also, the HNRC facility conditional risk ($R_C$) can be computed by the mentioned equation:

$R_C = [1 - (P_I \times P_N)] \times C$ where, C is the consequences, and C = from 0 to 1, according output results obtained from SAVI model, where $P_I$= 0.8975and $P_N$= 0.9200 so, the conditional risk will be $R_C = [1 - 0.8975 \times 0.9200] \times C$, then Rc= 0.18*C. Figure 17 shows the relationship graph between the conditional risk ($R_C$) and the consequences (C) of the hypothetical research reactor facility (HNRC). Sabotage scenario path #1 is the highest risk of all scenarios and the risk value depends on the C which is determined by the needs of regulations of the regulatorybody.




| Cosequences | 0 | 0.1 | 0.2 | 0.3 | 0.4 | 0.5 | 0.6 | 0.7 | 0.8 | 0.9 | 1 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Conditional Risk | 0 | 0.018 | 0.036 | 0.054 | 0.072 | 0.09 | 0.108 | 0.126 | 0.144 | 0.162 | 0.18 |

**Figure 17: The relationship graph between the conditional risk (RC) and the consequences (C).**

## Conclusion

This paper proposes an approach to planar target coverage analysis in sensor networks using Clifford algebra when the objective is seen as a two-dimensional surface. Clifford algebra is used to provide a formula that represents the plane target and the relationship between sensor nodes and the plane target. For a plane target, the maximal breach route algorithm is suggested. The weights of the point target and the plane target were compared. Through testing, the algorithm's efficacy was confirmed. Because the breach weight of the plane target is higher than the breach weight of the point target when there are the same number of sensor nodes. This is due to the fact that both the plane target's area and the sensor node's coverage area are taken into account when determining the maximum breach weight for the target. Higher-dimensional targets in sensor networks can be monitored using this technique. Additionally, non-omnidirectional sensor networks, including video sensor networks, may be included in the future because only omnidirectional sensor networks are employed in this article. That case will require further investigation.

Analysis and evaluation of security system is necessary and should be determined. In this work SAVI program was used in this evaluation and the 10 vulnerability entry paths to HNRC were determined. SAVI determines the most vulnerable path as a measure of system effectiveness, the effectiveness of the security system, $P_E$ along the worst vulnerability path was 82%, and this depends upon the probabilities of interruption, PI, and Neutralization $P_N$. The SAVI output results showed that $P_I$ is 0.89 which is sufficient and although $P_N$ is quite high 0.92. System probability of detection $P_D$ was 94%, and the need deployment response time is 45 seconds at the site and the response forces still have a time of 5 minutes to stop the terrorist and 130 seconds remaining after the neutralization of the adversary. This analysis concludes that the security system of HNRC facility is winning against the worst path of the terrorists attack and achieved its objective.

## References


- **Abo-Bakr, O.; Abdel-Rahman, M.A.E.; and El-Mongy, S.A. (2019):** Validation and Correction for 208Tl Activity to Assay 232Th in Equilibrium with Its Daughters. *Phys. Part. Nucl. Lett, 16(6):835.*
- **Akkaya, K.; and Younis, M. (2005):** A survey on routing protocols for wireless sensor networks. *J. Ad. Hoc. Networks. 3 (3):325*
- **Bonnah, E.; Ju, S.; and Cai, W. (2019):** Coverage Maximization in Wireless Sensor Networks Using Minimal Exposure Path and Particle Swarm Optimization. *Sens. Imaging, **21**(1):4.*
- **Breuils, S.; Tachibana, K.; and Hitzer, E. (2022):** New Applications of Clifford's Geometric Algebra. *Adv. App. Clifford Algebr, 32(2):17.*

- **EI-Kafas; A.E.; Wadood, A.A.; and Mansour, A.E. (2008):** Evaluation and Upgrading of the Physical Protection System of a Hypothetical Nuclear Facilities against Sabotage and Threat. *Arab J. Nucl. Sci. Appl, 41(3):313.*
- **Elsamahy, M.; Nagla, T.F.; and Abdel-Rahman, M.A.E., (2021):** Continuous online monitoring in pressurized water reactors during flexible operation using PLSR-based technique–Case study: Load following test. *J. Ann. Nucl. Energy, 161: 108473.*
- **Franchini, S.; Vassallo, G.; and Sorbello, F. (2017): A** brief introduction to Clifford algebra.*, https://www.researchgate.net/publication/228955605*
- **Garcia, M.L., (2007):** Design and Evaluation of Physical Protection Systems, *2nd. Edit. Butterw.Heinemann.*
- **Garcia, M.L., (2005):**Vulnerability Assessment of Physical Protection Systems. *Elsevier Sci. Butterw.Heinemann*
- **Gau, R.H.; and Peng.Yy. (2006):** A Dual Approach for The Worst-Case-Coverage Deployment Problem in Ad-Hoc Wireless Sensor Networks. *in IEEE Inter. Conf. MASS*
- **Gorain, B.; and Mandal, P.S. (2019):** Approximation Algorithms for Barrier Sweep Coverage. *Int. J. Found. Comput. Sci., **30** (03): p.425.*
- **Hao, Z.; Dang, J.; and Wang, X. (2021):** A node localization algorithm based on Voronoi diagram and support vector machine for wireless sensor networks. Int. J. Distrib. Sens. Netw, ***17**(2):1550147721993410.*
- **Hong, Y. et al., Hong, Y.i.; Yan, R.; Zhu,Y.; Li, D.; and Chen, W. (2017):** Finding best and worst-case coverage paths in camera sensor networks for complex regions. *J. Ad. Hoc. Netw., **56**:202.*
- **IAEA, Nuclear Security Series No. 13, (2011):** Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5), *IAEA. NS .Series. Vienna, Austria.*
- **Jondhale, S.R.; Maheswar, R.; and Lioret, J. (2022):** Fundamentals of Wireless Sensor Networks, in Received Signal Strength Based Target Localization and Tracking Using Wireless Sensor Networks, *S.R.; R.; J;, Editors., Springer: Cham. p.1*
- **Chang, J.; Yu, J.;Ke, J.; and Jingsong, H. (2010):** Simulation of worst and best-case coverage for wireless sensor network. *In. Inter. Conf .ICINA.2010.*
- **Kim, K.; and Lee, S. (2021):** Algorithms for Finding Vulnerabilities and Deploying Additional Sensors in a Region with Obstacles. *J. Electronics. **10**(12):.1504.*
- **Lee,.C.; Shin, D.; Bae, S.W.; and Choi, S. (2013):** Best and worst-case coverage problems for arbitrary paths in wireless sensor networks. *in The 7th IEEE Inter. Conf. MASS*
- **Macdonald, A., (2010):** A Survey of Geometric Algebra and Geometric Calculus. *Adv. App. Clifford Algebr, **27**(1): 853.*
- **Mahfouz, A.M.; Ismail, A.S.; El Sobky, W.I.; Nasry, H. (2023):** A novel model for representing a plan target and finding the worst-case coverage in wireless sensor network based on Clifford algebra. *EURASIP. J Wirel. Commun. Netw. **2023** (1):95.*
- **Mahfouz, A.; Zaky, H.; Ismail, A.; and Dahab, E. (2022):** Mathematical Model for Omnidirectional Sensor Network Using Clifford Algebra. J. Phys.: *Conf. Ser., 2304: 012001.*
- **Mahfouz A.M.; Ismail, A. S.; Zaky, H.; and Alsobky, W.I. (2022):** Path Detection for A Moving Target in Wireless Sensor Network Based on Clifford Algebra. *Inter. Conf. ITC-Egypt, 1-5.*
- **Mann, S.; and Dorst, L. (2002):** Geometric algebra: a computational framework for geometrical applications. *IEEE C. G. and A, **22**(4): 58.*
- **Matter, J.C., (1988): SAVI,** A Pc-Based Vulnerability Assessment Program. *SNL.Lab. Albuq. New-Mexico. USA.*
- **Meguerdichian, S.; Koushanfar, F.; QU, G.; and Potkonjak, M. (2001):** Exposure in wireless Ad-Hoc sensor networks, *in Proceedings of the 7th annual. Inter. Conf. MobiCom: Rome, Italy.139.*
- **Megerian, S.; Koushanfar, F.; Potkonjak, M.; and Srivastava, M.B. (2005):** Worst and best-case coverage in sensor networks. *IEEE Trans. Mob. Comput., **4**(1): 84.*
- **Nasry, H.; Xu, W.; Gong, J.W.; and Chen, H.Y. (2014):** Teleoperation Transparency Using Model Predictive Control. *J. AMM., 446-447: 115.*
- **Nasry, H. (2019):** Coordinate Transformation in Unmanned Systems Using Clifford Algebra. *Proceedings of the 5th Inter. Conf. ICMRE'19.*
- **Norichika,T. (2014):** Mitsutoshi, S. , A probabilistic extension of the EASI model. *J. P. S., **7**(2): 12.*
- **Oyeyinka, O.D.; Dim, L.A.; Echeta, M.C.;and Kuye, A.O. (2014):** Determination of System Effectiveness for Physical Protection Systems of a Nuclear Energy. *J. Sci.Technol. e-ISSN: 2163-2677.,4(2):9*
- **Ribeiro, M.G.; Neves, L.A.; Pinto, A.S.R.; and Nascimento, M.Z. (2015):** Surface Coverage in Wireless Sensor Networks

Based on Delaunay Tetrahedralization. *J. Phys.Conf. Seri,* ***574****:.012083.*

- **Rother, F.C.; Rebello, W.F.; Healy , M.J.F.; Silva , M.M.; Cabral, P.A.M.; Vital, H.C.; and Andrade, E.R. (2016):** Radiological Risk Assessment by Convergence Methodology Model in RDD Scenarios. *Risk Anal.,* ***36****(11): 2039.*
- **Taylor, M.D., (2021):** An Introduction to Geometric Algebra and Geometric Calculus. *[Online]. Available: https://books.google.com.eg/books?id=ajmWzgEACAAJ.*
- **Temene, N.; Sergiou, C.; Georgiou, C.; and Vassiliou, V. (2022):** A Survey on Mobility in Wireless Sensor Networks. *J. Ad. Hoc. Netw, 125: p.102726.*
- **Veltri, G., Huang, Q.; Gang Qu,G.; and Potkonjak, M. (2003):** Minimal and maximal exposure path algorithms for wireless embedded *Int. J. sens. netw. 40-50.*
- **Wadoud, A.A; Adail, A.S; and Saleh, A.A (2018):** Physical protection evaluation process for nuclear facility via sabotage scenarios. *Alex. Eng. J., 57 (2):831.*
- **Wadoud, A.A; El Eissawi, H.M; and Saleh, A.A (2017):** Protection of high ceiling nuclear facilities using photo-electric sensors and infrared fire detectors. *Arab J. Nucl. Sci. Appl., 50 (1):194.*
- **Wadoud, A.A; Agamy, S.; Gabal, H. A.; and Trabelsi, M. (2019):** Physical Protection System Evaluation and Consequences Analysis at Research Reactor Facility via Sabotage Scenarios" *J. Electr. Eng. Korea. ISSN. 1975-0102. (2020) 15:61*
- **Xie, W.; Cao, W.; and Meng, S. (2008):** Coverage analysis for sensor networks based on Clifford algebra. *Sci. in. China Seri. F: J. Inf. Sci.,* ***51****(5): p.460.*
- **Yi, Z.; and Chakrabarty, K. (2005):** A distributed coverage- and connectivity-centric technique for selecting active nodes in wireless sensor networks. *IEEE Trans. Comput.,* ***54****(8): 978.*
- **Zaky, H.N., Zaky, H.N.; Abd Elfatah, G.; El-Mongy, S.A.; and Abdel-Rahman. M.A.E. (2023):** Euler–Maruyama algorithm in estimating UGV path and location in nuclear emergency and security applications*. J. Kerntechnik.,* ***88****(3):361.*