Article

Not peer-reviewed version

Aperiodic Tiling for Enhancing Security in Wireless Sensor Networks

Ayaz Khan * , Gabriel Macias-Villegas , Habib M. Ammari

Posted Date: 21 August 2024

doi: 10.20944/preprints202408.1495.v1

Keywords: wireless sensor networks; clone attacks; intrusion detection; security topology

 doi:10.20944/preprints202408.1495.v1

Article

Aperiodic Tiling for Enhancing Security in Wireless Sensor Networks

Ayaz Khan [1,*], Gabriel Macias-Villegas [2] and Habib M. Ammari [3]

[1] CUNY Hunter College
[2] University of Nebraska - Lincoln
[3] Texas A&M - Kingsville
* Correspondence: ayaz.khan04@myhunter.cuny.edu

Abstract: This paper investigates the impact of network topologies on the security of wireless sensor networks (WSNs). We propose the use of Spectre Monotile aperiodic tiling for sensor deployment, demonstrating its superior security compared to regular deterministic topologies. Additionally, we introduce a novel Intrusion Effort Index to quantify network resilience against clone attacks. By implementing a smart random walk to simulate the scenario of malicious cloned nodes attempting to reach the central access point of a network, we take into consideration the worst-case scenario for a network as it is being attacked. Given all network topologies use the same intrusion detection system and security protocols, we discover the topology of a network will also play a role and provide an additional layer of security depending on how it is designed. Similar to a fog-of-war, the sensor positions play a vital role in how an intruder assesses a network. By tiling a plane non-periodically, an absence of regularity in the structure is produced, which obfuscates an intruder attempting to predict the next sensor position, due to a varying number of adjacent neighboring nodes each time it reaches a new node. After 10,000 rounds of simulation emulating different scenarios of malicious nodes compromising the network, we averaged the results to find total detections, total hops, and percentage of times the base station was reached. Our simulation results show that aperiodic tiling has the best security resilience and robustness compared to other flat network topologies.

Keywords: Wireless Sensor Networks (WSNs); aperiodic tiling; spectre monotile; intrusion detection; network topologies; clone attacks

---

1. Introduction

1.1. Background and Motivation

1.1.1. Overview of Wireless Sensor Networks

Wireless sensor networks (WSNs) comprise a collection of sensor nodes that intercommunicate, transmit, and exchange information via signals. These networks are crucial for applications such as global information exchange. Deployed over vast and often un-monitored areas, WSNs are vulnerable to intrusion, making robust security measures essential to ensure their longevity. A major goal is to ensure WSNs are able to withstand intrusion attacks under different scenarios and conditions.

1.1.2. Importance of Security in WSNs

Traditional network topologies, such as hexagonal, triangular, and square grids, have been widely used in WSN applications due to the their ease of deployment and uniform coverage. However, these deterministic patterns are vulnerable to attacks as they make sensor placements predictable. This leads to sub-optimal coverage and weak security within networks. Our focus is on enhancing the robustness and resilience of WSNs through utilizing and exploiting the aperiodic properties in tiling, particularly examining the relationship between sensor deployment and security strength.

 doi:10.20944/preprints202408.1495.v1

1.1.3. Advantages of Aperiodic Tiling

Tessellation of a 2D plane using periodic and aperiodic schemes reveals hidden solutions by leveraging the properties of the shapes used. While periodic tiling has been extensively studied [1], aperiodic tiling offers unique benefits for WSNs. Aperiodic patterns, which never repeat exactly, create complex and non-uniform structures that enhance security through unpredictability in sensor placement. These patterns exhibit self-similarity, maintaining consistent structural properties regardless of network size, and providing network resilience against targeted attacks. Aperiodic tilings can be applied to irregular terrains, offering greater flexibility in real-world deployments. This makes aperiodic tiling a promising approach for improving the security and resilience of WSNs. The significance of aperiodic tiling was highlighted by Roger Penrose in the 1970s with his discovery of the "kites and darts" shapes, which demonstrated that simple shapes could create infinitely complex, non-repeating patterns. Innovations such as the "spectre" monotile have deepened our understanding by simplifying the creation of aperiodic tiling to one tile while preserving its intricate properties.

1.2. Problem Statement

WSNs are indispensable in applications such as environmental monitoring, health surveillance, and military operations due to the capabilities of data collection and transmission. It is essential that we ensure the security of these networks since any breach may result in major loss of information and faults.

1.2.1. Security in WSNs

Traditional security methods in WSNs, which depend primarily on Intrusion Detection Systems (IDS) and different security protocols, are frequently ineffective in isolation due to the constantly changing and unpredictable nature of WSN deployment scenarios. In order to develop a more durable and resilient network architecture, additional layers of security must be added that go beyond traditional IDS and protocols. This necessity is heightened by the fundamental restrictions of sensor nodes, such as limited computing and energy resources, making it desirable to achieve both coverage through tiling and security with irregular patterns in one go.

1.2.2. Impact of Network Topologies on Security

The topology of a WSN is a critical aspect in its security. Conventional network topologies, such as hexagonal, triangular, and square grids, are predictable and easily abused by attackers who leverage the network structure. This predictability affects the viability of security mechanisms since hackers can theoretically weaken them by exploiting recurring patterns. In contrast, deploying sensor nodes with aperiodic tiling, such as the Spectre Monotile pattern, introduces unpredictability and complexity. Aperiodic tiling hampers the prediction of sensor locations, enhancing security by making it harder for attackers to plan and execute attacks. This additional layer of defense supplements standard security techniques and helps to create a more secure WSN system.

1.3. Contributions and Structure of the Paper

This paper presents several key contributions to the field of WSNs, focusing on enhancing security. We introduce the Spectre Monotile aperiodic tiling pattern for sensor deployment, an innovative approach that enhances network security by introducing unpredictability and complexity in sensor placements, making the network more resilient to targeted attacks. We develop the Intrusion Effort Index (IEI), a novel metric designed to evaluate the effort required for an intruder to compromise the network, considering factors such as the distance traveled by the intruder, the complexity of the network layout, and the total number of sensors being used.

Extensive simulations are conducted to evaluate the proposed methods' performance, encompassing various network scenarios and configurations to test the robustness, deployment, and security

 doi:10.20944/preprints202408.1495.v1

resilience of the WSN. The results provide practical insights into the application of aperiodic tiling in real-world WSN deployments.

The remainder of the paper is organized as follows: Section II covers relevant work in the area of WSN security, particularly existing approaches regarding network topologies and security techniques. Section III provides preliminary information on network structures, simulations parameters, and Spectre monotile tiling. Section IV explains mathematical underpinnings and terms. Section V discusses the methodology employed to implement the Smart Random Walk Cloned Nodes Intruder Simulation and the Intrusion Effort Index. Section VI presents and investigates the findings, particularly security metrics such as, base station reach percentage, total intrusion effort, average compromised nodes, and average detections.

2. Related Work

2.1. Security of WSNs

Most papers regarding security revolve around the scenario on what a network designer should do given a breach has occurred. We take inspiration from existing papers but go a step further by answering the question: What should be done to ensure a breach never results in the entire network collapsing? We use similar security approaches and display scenarios from both ends: the intruder's and the designer's.

To begin with, the tiling being used in the paper is courtesy of Smith et al. [2]. They devised a method of using a single tile to tile aperiodically perpetually; this trait makes it a good fit for our case of testing it against homogeneous WSNs. By already having proven the tile's aperiodicity, our results are further supported when its aperiodic property boosts our security affirmations.

Several researchers have focused on the development of secure WSN architectures. Birjandi et al. [3] discussed k-coverage in regular deterministic sensor deployments, highlighting the importance of coverage in enhancing network security. Chen et al. [4] proposed a security topology protocol based on community detection and energy-aware mechanisms, addressing both security and energy efficiency in WSNs.

Bysani and Turuk [5] conducted a comprehensive survey on selective forwarding attacks in WSNs, identifying the vulnerabilities and proposing countermeasures to mitigate such attacks. Keerthika and Shanmugapriya [6] examined active and passive attacks on WSNs, detailing various vulnerabilities and the corresponding countermeasures.

Butun et al. [7] surveyed IDS in WSNs, providing a detailed analysis of existing IDS approaches and their effectiveness in detecting different types of attacks. Ammari [1] explored the use of hexagonal tiling to achieve sensing k-coverage, discussing the implications of such tiling patterns on network security and coverage.

Zeng et al. [8] introduced a random-walk based approach to detect clone attacks in WSNs, emphasizing the importance of randomness in enhancing network security. Liu et al. [9] investigated strong barrier coverage in WSNs, proposing methods to ensure robust coverage and prevent unauthorized access.

Luo et al. [10] developed a mechanism for detecting selective forwarding attacks and recovering the network using cloud-edge cooperation in software-defined WSNs. Shahzad et al. [11] surveyed active attacks on WSNs, discussing various attack types and proposing countermeasures to enhance network security.

Aalsalem et al. [12] proposed a constrained random walk approach to detect clones in WSNs, further supporting the use of randomness and unpredictability in securing sensor networks.

In summary, the existing body of work highlights the significance of secure network topologies and the use of advanced algorithms to enhance the security and efficiency of WSNs. While existing research focuses on the Intrusion Detection System (IDS) of a given network topology, our paper analyzes how the topology itself contributes to the security. This paper builds on these foundations by introducing the Spectre Monotile aperiodic tiling pattern, developing a novel Intrusion Effort Index,

 doi:10.20944/preprints202408.1495.v1

and presenting a smart random walk security attack simulation, thereby addressing key security and deployment challenges in WSNs.

2.2. Network Topologies in WSNs

The topology of a WSN plays a crucial role in determining its efficiency, coverage, and security. Various topologies have been studied and implemented in WSNs, each with its advantages and disadvantages.

2.2.1. Periodic Topologies

Traditional WSNs often employ regular, deterministic topologies such as hexagonal, triangular, and square grids due to their simplicity and ease of deployment.

***Hexagonal Grid Topology*:** Hexagonal grids provide an efficient way to achieve uniform coverage with minimal overlap between sensor nodes. This topology is often used in applications requiring consistent coverage and efficient use of resources. However, its predictability can make it vulnerable to security breaches, as attackers can easily map out sensor positions [1].

***Triangular Grid Topology*:** Triangular grids are another common topology that offers good coverage and connectivity. The equilateral triangle arrangement allows for efficient communication between nodes, but like hexagonal grids, the regular pattern may be exploited by attackers.

***Square Grid Topology*:** Square grids are simple to deploy and manage, making them popular in many WSN applications. They provide good coverage and high fault-tolerance, but can suffer from the same predictability issues as hexagonal and triangular grids, making them less secure against targeted attacks.

2.2.2. Security Methods in WSNs

The application of aperiodic tiling in WSNs is a relatively new area of research, but it has shown significant potential in improving network security and efficiency from our findings. Researchers have at least understood how randomness or irregularity plays a direct role in the efficacy of deployment in security overall.

***Random Walk Approaches*:** Zeng et al. [8] proposed a random-walk based approach to detect clone attacks in WSNs, emphasizing the importance of randomness in enhancing network security.

***Strong Barrier Coverage*:** Liu et al. [9] investigated strong barrier coverage in WSNs, highlighting the advantages of complex, non-uniform patterns in preventing unauthorized access.

In conclusion, the use of aperiodic tiling, such as the Spectre Monotile pattern, presents a promising approach to enhancing the security and efficiency of WSNs. By introducing complexity and unpredictability in sensor placements, aperiodic tiling can significantly improve network resilience against targeted attacks, making it a valuable addition to the design of secure WSN architectures.

3. Preliminary Information

3.1. Network Topologies

In this study, we tie in the problem of achieving k-coverage in deterministic homogeneous sensor deployments, as detailed in the work by Birjandi et al. [3] with barrier coverage by Kumar et al. [13] in WSNs. The focus is on forming a relationship between coverage in regular deterministic sensor deployments, and how it directly affects security resilience overall. We then show how the combination of unique angles and unique distances in a topology directly affects security, and how aperiodic tiling excels. The terms in Table 1 will clarify and help with understanding for the next sections.

 doi:10.20944/preprints202408.1495.v1

Table 1. Terminology and Definitions.

Term	Definition
Sensor Density	The number of sensors per unit area at least 1-covered in a WSN.
Rate of Overlap	The percentage of area covered by multiple sensors.
Spectre Supertile Area	The total area covered by the Spectre Monotile aperiodic tiling pattern.
Total Intrusion Effort (Ω)	The cumulative effort required for an intruder to compromise the network, considering factors such as distance traveled and spatial complexity of the network layout.
Smart Random Walk	A postulate assumed for the intruder to move within the network, hopping from one unvisited node to another without failure, but with chances of detection.
Complexity Factor	A measure of the complexity of the network layout, calculated based on unique angles and distances between nodes. Higher complexity factors indicate more unpredictable and secure network structures.

3.1.1. Security

Our research indicates that the type of coverage over a region directly affects the likelihood of intruder detection, thereby enhancing security resilience. For fixed regular deterministic sensor deployments (triangles, squares, hexagons), we observe a consistent level of security that is inherently dependent on the network topology. Specifically, in a regular deterministic WSN, any arbitrary node (excluding boundary nodes) has a fixed number of neighboring nodes at predetermined distances and angles. This regularity in the network structure can potentially simplify an intruder's efforts when traversing the network in attempts to reach the sink or base station. The predictable nature of these topologies may inadvertently provide advantageous information to potential intruders, allowing for more efficient navigation through the sensor field. This finding underscores the importance of considering topology variability in WSN design to enhance overall network security.

***Security Implications of Network Structures*:** Triangles: In comparison with hexagons and squares, offers the best amount of intrusion effort due to a higher number of neighboring nodes at smaller unique angle increments. Hexagons: Present intermediate difficulty for intruders due to fewer neighbors but the hop distance is greater since more area is covered, hence better than the square. Squares: Provide the easiest path for intruders due to a low number of neighboring nodes and at fixed angles, the vertical and horizontal symmetry is easily exploited.

***Correlation Between Topology and Network Resilience*:** The distance between neighboring nodes and their corresponding angles directly affect the network's security. Moreover, the fault-tolerance over an area or region and the amount of area being covered are also factors for intrusion effort which will be seen in subsequent results.

3.1.2. Aperiodic Network Topology

As shown in Figure 1, the coverage map for Spectre aperiodic tiling achieves a minimum of 1-coverage throughout, with areas of redundancy where regions are 2, 3, or at most 4-covered. This contrasts with regular tilings where hexagons and triangles have regions that are at most 2-covered, and squares have multiple regions that are 4-covered. The impact of these coverage differences on security metrics will be discussed in the subsequent sections.

 doi:10.20944/preprints202408.1495.v1

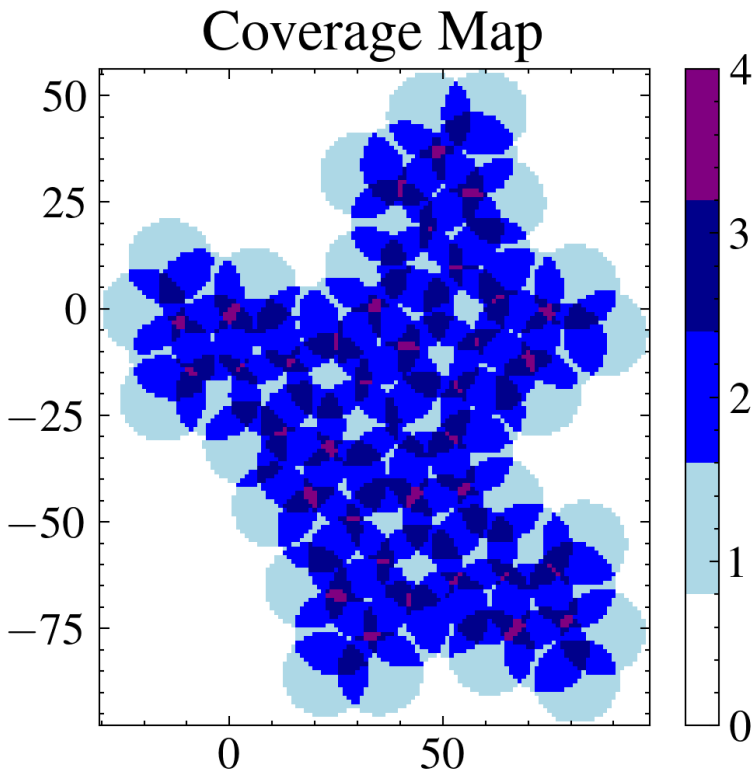

Figure 1. Coverage Map for 71 Sensors.

3.1.3. Barrier Coverage in WSNs

The work by Kumar et al. [13] primarily discusses the concept of barrier coverage in WSNs. Key contributions and concepts that relate to our hypothesis include:

***Barrier Coverage Definition*:** Introduces α-barrier coverage to measure the quality of coverage, ensuring that every path crossing the barrier intersects the sensing area of at least one sensor. This concept directly supports our hypothesis that higher coverage levels increase the probability of intruder detection.

***Algorithms and Models*:** Provides algorithms for constructing α-barrier coverage using sensors, which determine the optimal placement of sensors to maximize coverage and, consequently, security. These models reinforce the idea that strategic deployment enhances detection capabilities.

Performance Metrics Focuses on the number of sensors required and their deployment patterns to achieve α-barrier coverage. The analysis of sensor density and its impact on barrier coverage aligns with our hypothesis that higher sensor density (or coverage) directly correlates with increased security and resilience against intrusions.

Kumar et al.'s findings [13] emphasize the critical role of sensor density and strategic deployment in achieving effective barrier coverage. This aligns with Birjandi et al. [3], who also highlight the importance of optimal sensor placement for achieving k-coverage. Both studies focus on different topics, however, there is a relationship that can be seen between redundant coverage (or k-coverage) which is directly correlated with the levels of security detection.

Furthermore, the study's discussion on critical and strong α-barrier coverage models provides insights into how different levels of coverage affect the network's ability to detect intrusions. Strong α-barrier coverage guarantees detection of all intruders, indicating that higher coverage levels (more sensors) significantly enhance security resilience.

 doi:10.20944/preprints202408.1495.v1

3.2. Simulation Setup

3.2.1. Simulation Environment

Simulations are conducted using Python with libraries for numerical computations and visualizations. The parameters are chosen to reflect realistic WSN deployments.

Parameters and Assumptions

- *Network configurations*: Periodic Schemes as hexagonal, triangular, square, and aperiodic Spectre Monotile.
- *Uniform detection*: All sensors have a uniform probability of detecting an intrusion.
- *Sensing range*: The sensing range of each sensor is set to 10 units.
- *Communication range*: The communication range is twice the sensing range.
- *Static sensors*: Sensors are assumed to be static after deployment.

3.3. Spectre Monotile Tiling

3.3.1. Introduction to Spectre Monotile

The Spectre Monotile, discovered by Smith et al. [2], exhibits aperiodic properties that prevent exact repetition, providing superior security characteristics by introducing unpredictability in sensor placements.

3.3.2. Application in WSNs

Sensor deployment strategies involve placing sensors at the centroids of the Spectre Monotile tiles to maximize coverage and minimize predictability. This approach leverages the self-similarity and non-repetitive nature of aperiodic tiling.

4. Terminology

4.1. Mathematical Framework

This section presents the mathematical foundation for the key processes used in evaluating the security metrics of WSNs using aperiodic and regular tiling methods. It should be mentioned that the Spectre tiling works in iterations based on its hierarchical substitution rule [2]. In other words, depending on the number of tiles (or in our case, number of sensors) being placed, we have a fixed number of sensors. Via iterations, the number of sensors being used will be: 9, 71, 556, 4401, etc. For our analysis, we are using iteration 2, which is 71 sensors Figure 2. The change in iteration only slightly changes the sensor density, but on average it will be 0.006 when sensor radius is 10. For comparison, the sensor density for triangular tiling is 0.024, square tiling is 0.010, and hexagonal tiling is 0.004. As the iteration gets bigger, so does the Spectre supertile area. All other metrics remain constant even with change in iteration.

Definition 1 (**Coverage Calculation**). *The coverage map of Spectre tiling as seen in Figure 2; the sensor network is calculated based on sensor positions and sensing radii.*

$$C(x,y) = \sum_{i=1}^{N} \mathbf{1}_{\|\mathbf{s}_i-(x,y)\|\leq r} \tag{1}$$

where:

- $C(x,y)$ *is the coverage function at the point* (x,y).
- N *is the total number of sensors in the network.*
- $\mathbf{s}_i$ *is the position vector of the i-th sensor.*
- (x,y) *is the position vector of the point being evaluated for coverage.*
- r *is the sensing radius of each sensor.*

 doi:10.20944/preprints202408.1495.v1

- $\|\mathbf{s}_i - (x,y)\|$ *is the Euclidean distance between the i-th sensor and the point* (x,y).
- $\mathbf{1}_{\|\mathbf{s}_i-(x,y)\|\leq r}$ *is an indicator function that equals 1 if the point* (x,y) *is within the sensing radius r of the i-th sensor, and 0 otherwise.*

This function determines the areas covered by the sensors, with respect to the field it is deployed; it is imperative to calculate this for determining sensor density and also since Spectre tiles irregularly and hence a regular grid will leave areas that are not covered. Here, s_i *is the random variable representing the sensor positions, and the summation ensures that we count all points within the sensing radius of any sensor.*

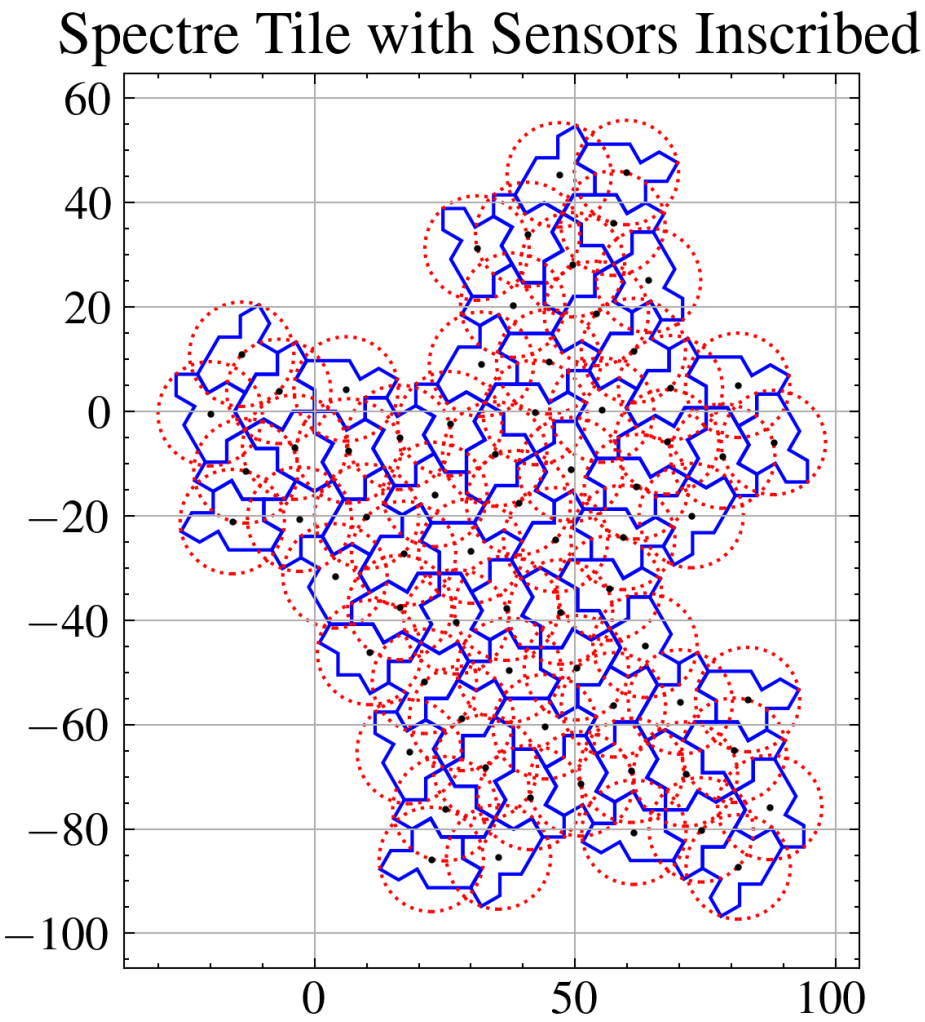

Figure 2. Spectre Tile Inscribed for Sensor Coverage.

Definition 2 (Network Metrics Calculation). *Various metrics are calculated to evaluate the performance and efficiency of the sensor network. These metrics were taken from [1], and are introduced to standardize and establish coverage to prove the Spectre tiling can be used to deploy a WSN.*

Sensor Density*:*

$$\rho = \frac{N}{A} \tag{2}$$

where N is the number of sensors and A is the covered area.

Rate of Overlap*:*

$$R_o = \frac{A_c - A_t}{A_c} \tag{3}$$

where A_c *is the circle area, and* A_t *is the tile area.*

 doi:10.20944/preprints202408.1495.v1

These metrics are standardized metrics used to understand how good a topology performs in comparison with the typical square, triangle and hexagonal arrangements.

4.2. Proofs and Theorems

Given a regular deterministic wireless sensor network topology, an arbitrary node (provided it is not a boundary/fence node), will have a fixed number of neighboring nodes at fixed angles, which can be observed throughout the network topology in repeating patterns.

Proof. We will prove this conjecture for three common regular deterministic sensor network topologies: square grid, triangular grid, and hexagonal grid.

Square Grid

- *Node Arrangement*: Nodes are placed at regular intervals along orthogonal axes, forming a square lattice.
- *Neighbors*: Each node (excluding boundary nodes) has 4 neighbors.
- *Angles*: The neighbors are located at 90-degree angles relative to each other.

To formalize, consider a node at coordinates (i, j). Its neighbors are at $(i+1, j)$, $(i-1, j)$, $(i, j+1)$, and $(i, j-1)$. This pattern repeats across the entire grid, confirming the conjecture for the square grid.

Triangular Grid

- *Node Arrangement*: Nodes are placed such that each node is equidistant from its six nearest neighbors, forming a pattern of equilateral triangles.
- *Neighbors*: Each node (excluding boundary nodes) has 6 neighbors.
- *Angles*: The angles between consecutive neighbors are 60 degrees, forming a pattern of equilateral triangles.

To formalize, consider a node at coordinates (i, j). Its neighbors can be calculated as follows:

$$\begin{aligned} (i \pm 1, j), &\quad \text{(direct neighbors to the left and right)}, \\ (i \pm 1/2, j \pm \sqrt{3}/2), &\quad \text{(neighbors offset by 60 degrees)}. \end{aligned}$$

This arrangement forms a repeating pattern of equilateral triangles across the grid, confirming the conjecture for the triangular grid.

Hexagonal Grid

- *Node Arrangement*: Nodes are arranged such that each node is equidistant from its six nearest neighbors, forming a pattern of regular hexagons.
- *Neighbors*: Each node (excluding boundary nodes) has 6 neighbors, similar to the triangular grid.
- *Angles*: The angles between consecutive neighbors are still 60 degrees, but the overall structure forms hexagons rather than triangles.

To formalize, consider a node at coordinates (i, j). Its neighbors can be calculated similarly to the triangular grid:

$$\begin{aligned} (i \pm 1, j), &\quad \text{(direct neighbors to the left and right)}, \\ (i \pm 1/2, j \pm \sqrt{3}/2), &\quad \text{(neighbors offset by 60 degrees)}. \end{aligned}$$

However, the crucial difference is in the arrangement pattern, where these nodes form a hexagonal tiling rather than triangular. The repeating pattern of hexagons ensures that each node has the same fixed number of neighbors at fixed angles.

Difference between Triangular and Hexagonal Grids: - While both the triangular and hexagonal grids have nodes with 6 neighbors at 60-degree angles, the key difference lies in the overall pattern they form: - In the triangular grid, the nodes form a pattern of equilateral triangles, leading to a more connected and denser network. - In the hexagonal grid, the nodes form a pattern of hexagons, which is less dense but provides a uniform distribution of neighbors.

 doi:10.20944/preprints202408.1495.v1

This distinction is crucial when analyzing network properties such as coverage, connectivity, and intrusion detection.

In all three cases, we see that an arbitrary node has a fixed number of neighboring nodes at fixed angles, and this pattern repeats throughout the network. Thus, the conjecture holds for regular deterministic wireless sensor network topologies.

□

5. Methodology

5.1. Smart Random Walk Cloned Nodes Intruder Simulation

5.1.1. Existing Approaches

There have been multiple papers on how to truly emulate and design a security simulations. Aside from computational challenges and time complexity issues, it becomes quite difficult to simulate how an intrusion would work since there is no verifiable practical data that can be annotated. This in turn have made researchers to opt for theoretical solutions, ranging from working on the best form of security via encryption, or outlaying the best security protocols to terminate an intruder. However, some works showcases simulations to their best extent with given assumptions and parameters.

5.1.2. Random Walk Approaches

Random walk methods simulate an intruder's movement through the network using probabilistic models. In these simulations, the intruder randomly selects the next node to move to, based on certain probabilities. This approach is straightforward and computationally efficient, making it suitable for large-scale simulations and is what we will be using in our paper. Other papers have used random walk as a means of detecting cloned nodes via collisions in signals, whereas we presume a smart random walk to showcase how cloned nodes compromise other nodes at random [8].

5.1.3. Graph-based Methods

Graph-based techniques represent the network as a graph, where nodes correspond to sensors and edges represent communication links. Graph theories capture the possible paths taken by an intruder, similar to what we are trying to showcase in terms of network topology. They can provide detailed insights into potential attack paths and vulnerabilities. For instance, leveraging Graph Neural Networks (GNNs) enables capturing complex interactions and topological structures within WSNs effectively. However, GNN-based methods don't account on a granular level like unique angles and distances, and a clear quantity isn't mentioned like the IEI for mathematical comparison [14].

5.1.4. Hardware and Software Considerations

Hardware and software limitations are a critical factor when assessing a network's security. Alongside, key components like energy consumption, firmware, bit-rate and data packet transmissions are also taken into consideration. However, this doesn't provide insight on network topologies themselves and how it should also change the trajectory of intruder behavior. Though there are metrics that show the difference in energy consumption dependent on topology, there is no clear outline on the advantage of the intruder if they were to test the network topology themselves [15].

Moreover, predictability is a major concern. Regular patterns in network topologies can make it easier for intruders to anticipate sensor placements and plan their attacks effectively. Existing simulations often fail to adequately address how introducing topological irregularities can enhance security by making it harder for attackers to predict network defenses. Thus, enhancing scalability, realism, and unpredictability in simulations is crucial for improving the overall effectiveness of network security strategies.

 doi:10.20944/preprints202408.1495.v1

5.1.5. Smart Random Walk Simulation Algorithm

The Smart Random Walk Simulation Algorithm 1 models the behavior of an intruder attempting to navigate through the network to reach the base station. Unlike traditional methods, this algorithm assumes the intruder is strategic, making decisions based on the network layout to prioritize visiting the nearest neighboring node. The algorithm can be outlined as follows:

Algorithm 1 Smart Random Walk Simulation

Require: Network $G = (V, E)$, Cloned node positions C, Base station B
Ensure: Detection metrics, Paths, Intrusion effort, Compromised nodes

Initialize $detections \leftarrow 0$
Initialize $paths \leftarrow$ empty list
Initialize $intrusion\_effort \leftarrow 0$
Initialize $total\_hops \leftarrow 0$
$compromised\_nodes \leftarrow$ set of clone positions C
$active\_clones \leftarrow$ set of clone positions C
Initialize $detected\_clones \leftarrow$ empty set
while $active\_clones$ is not empty **do**
  $new\_active\_clones \leftarrow$ empty set
  for each $clone\_position$ in $active\_clones$ **do**
    if $clone\_position$ is in $detected\_clones$ or has_reached_base_station($clone\_position$, B) **then**
      continue to next $clone\_position$
    end if
    Initialize $path \leftarrow [clone\_position]$
    Initialize $visited\_nodes \leftarrow$ empty set
    while $clone\_position \neq B$ **do**
      Add $clone\_position$ to $visited\_nodes$
      $next\_position, effort\_of\_intrusion, pattern\_found \leftarrow smart\_random\_walk(G, clone\_position, visited\_nodes)$
      if $next\_position$ is None or distance between $clone\_position$ and $next\_position > COMMUNICATION\_RANGE$ **then**
        break out of the loop
      end if
      $clone\_position \leftarrow next\_position$
      Add $clone\_position$ to $compromised\_nodes$
      Append $clone\_position$ to $path$
      $intrusion\_effort \leftarrow intrusion\_effort + effort\_of\_intrusion$
      $total\_hops \leftarrow total\_hops + 1$
      if random detection probability $< DETECTION\_THRESHOLD$ **then**
        Add $clone\_position$ to $detected\_clones$
        $detections \leftarrow detections + 1$
        break out of the loop
      end if
      if $clone\_position = B$ **then**
        break out of the loop
      end if
    end while
    Append $path$ to $paths$
    if $clone\_position$ is not in $detected\_clones$ and has not reached B **then**
      Add $clone\_position$ to new_active_clones
    end if
  end for
  $active\_clones \leftarrow new\_active\_clones$
end while
return $detections$, $paths$, $intrusion\_effort$, $total\_hops$, $detected\_clones$, number of $compromised\_nodes$

 doi:10.20944/preprints202408.1495.v1

Algorithm 1 - Parameters

- *Sensor Number*: The number of sensors being used.
- *Communication Range*: The maximum distance within which sensors can communicate with each other
- *Detection Threshold*: The probability range of detecting an intruder at each sensor.
- *Clone Percentage*: The percentage of nodes in the network that are cloned at random initial positions.

Simulation Process

- *Initialization*: The network is initialized with a predefined topology, and sensor nodes are placed according to the chosen pattern.
- *Clone Placement*: A percentage of sensors are designated as cloned nodes. These clones prioritize moving to the nearest unvisited neighboring node from its starting position, eventually hoping to reach the base station.
- *Intruder Movement*: The cloned nodes perform a smart random walk, moving from one node to the next based on the network's layout. The algorithm evaluates each possible move, considering factors like the distance to the next node, the number of hops, and the likelihood of detection.
- *Intrusion Effort Calculation*: As clones move through the network, their paths are tracked, and the total intrusion effort is calculated. This includes the number of hops taken, the total distance traveled, and the complexity of the path (unique angles and distances).

5.2. Intrusion Effort Index (IEI)

IEI Algorithm 2 is a novel metric designed to quantify the effort required for an intruder to navigate through a WSN and reach the base station. The IEI takes into account various factors that influence the difficulty of intrusion, providing a comprehensive measure of network security.

Factors Considered

- *Distance Traveled by Intruders*: The total distance that an intruder must cover to reach the base station. Longer distances typically indicate higher effort.
- *Complexity of Network Layout*: This includes the number of unique angles and unique distances between nodes, reflecting the unpredictability and complexity of the network's structure.
- *Size of Network*: The more nodes there are, the more paths, and hence the more the intrusion effort required for an intruder. It also increases the total number of boundary nodes hence producing more unique angles and unique distances; thus higher intrusion effort.
- *Number of Cloned Nodes*: The IEI is directly reflective of the total possible paths an intruder can make within a network, so it is reliant on the network size and also the number of intruders themselves as we add up to make the total intrusion effort.

Definition 3. *IEI is defined as:*

$$\Omega = \sum_{i=1}^{N} \left(\frac{d_i}{R} + \frac{1}{\theta_i} \right) \tag{4}$$

- Ω is the total intrusion effort.
- N is the total number of hops or movements made by the intruder.
- d_i is the distance traveled in the i-th hop.
- R is the sensing range of the sensors.
- θ_i is the angle between the current node and the next node in the i-th hop.

- *Distance Component*: The term $\frac{d_i}{R}$ represents the normalized distance traveled by the intruder in each hop. This normalization ensures that the intrusion effort is proportional to the distance relative to the sensor's sensing range.
- *Angle Component*: The term $\frac{1}{\theta_i}$ reflects the complexity introduced by the unique angles in the network. Smaller angles (indicating more complex paths) contribute more to the intrusion effort, emphasizing the difficulty of navigating through a network with irregular angles.

 doi:10.20944/preprints202408.1495.v1

– *Summation*: The total intrusion effort Ω is obtained by summing the contributions from all hops. This cumulative approach ensures that both the distance and the complexity of the path are accounted for in the final measure.

5.2.1. Significance of IEI in Network Security

The IEI provides a quantitative measure of the network's resilience against intrusions. By capturing both the physical and structural complexity of the network, the IEI offers a comprehensive assessment of how difficult it is for an intruder to reach the base station. This metric is crucial for evaluating and comparing the security of different network topologies.

5.2.2. Comparative Analysis of Network Topologies

The IEI can be used to compare the security of various network topologies, such as hexagonal, triangular, square, and aperiodic tiling. Networks with higher IEI values are considered more secure as they require more effort for an intruder to compromise. This comparison allows network designers to select topologies that offer optimal security for their specific applications.

Design and Deployment

– *Topology Selection*: By evaluating the IEI of different topologies, designers can choose the most secure layout for their network, balancing between security, coverage, and energy efficiency.
– *Sensor Placement*: The IEI helps in determining optimal sensor placements that maximize detection probabilities and increase the complexity of potential intrusion paths.
– *Security Protocols*: While traditional security measures focus on detection and response, the IEI integrates the network's inherent structural properties into the security evaluation, providing a more holistic approach to WSN security.

In conclusion, the Intrusion Effort Index is a powerful quantifiable metric used for ascertaining the "amount" of security for a network topology based on its spatial complexity and deployment. Because of this, the results showcase that the IEI is a reasonable value for understanding the amount of effort that would be exerted by an intruder when performing selective forwarding attacks.

Algorithm 2 Intrusion Effort Index Calculation

Require: Network $G = (V, E)$, Current node c
Ensure: IEI
$unique\_angles \leftarrow$ empty set
$unique\_distances \leftarrow$ empty set
for each node $n \in G$ **do**
  if $n \neq c$ **then**
    $distance \leftarrow \|n - c\|$
    Add $distance$ to $unique\_distances$
    $angle \leftarrow \text{atan2}(n.y - c.y, n.x - c.x)$
    Convert $angle$ to degrees and normalize to [0, 360)
    Add $angle$ to $unique\_angles$
  end if
end for
$complexity\_factor \leftarrow \text{len}(unique\_angles) + \text{len}(unique\_distances)$
$total\_distance \leftarrow \sum_{n \in G, n \neq c} \|n - c\|$
$IEI \leftarrow \frac{total\_distance}{SENSOR\_RADIUS} \times complexity\_factor$
return IEI

 doi:10.20944/preprints202408.1495.v1

6. Results and Discussion

6.1. Base Station Reached Percentage

6.1.1. Analysis of Different Topologies

The base station reached percentage is a critical metric that indicates the success rate of an intruder reaching the base station. This analysis is essential to understand how different network topologies impact the likelihood of successful intrusions. Our simulations were conducted over 10,000 rounds using an equal number of 71 sensors for all network designs to ensure statistical significance and to account for variability in intruder behavior and network responses while establishing a fair comparison in terms of energy usage and cost. The results are averaged to provide a robust assessment of each topology's performance.

6.1.2. Square Topology

The Square topology Figure 3 shows the highest base station reached percentage, indicating it is the least secure among the topologies tested. The simple and predictable grid layout allows intruders to easily map out sensor positions and plan efficient routes to the base station. Despite having a higher rate of overlap and redundancy, the regularity of the square pattern makes it easier for intruders to navigate through the network with minimal detection. The straightforward paths and fewer unique angles in a square grid reduce the complexity faced by the intruder, resulting in a higher success rate. Essentially, the square topology can be reduced and symmetric vertically and horizontally; this symmetry makes it the simplest to be exploited and reach the base station.

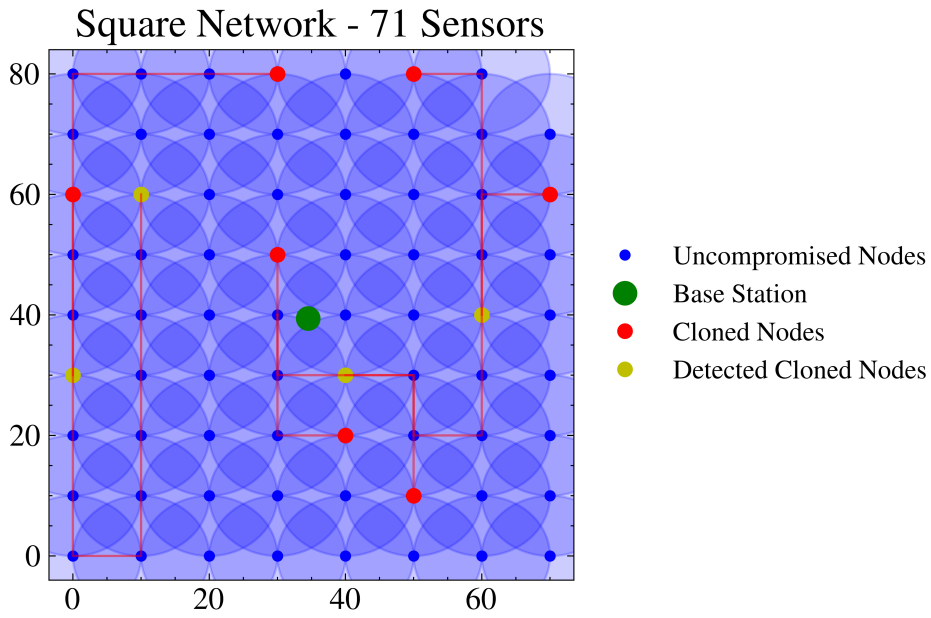

Figure 3. Square Network.

6.1.3. Hexagonal Topology

The Hexagonal topology Figure 4 exhibits a moderate base station reached percentage. The uniform hexagonal pattern provides good coverage and multiple unique angles, contributing to a balanced detection capability. However, its regularity can be exploited by intruders that can predict sensor placements based on the repeating pattern. As the hexagonal topology covers the greatest area, despite having the largest angles, it still has a good number of neighboring nodes and most importantly has the greatest hop distance, hence why it has a better intrusion effort than square.

 doi:10.20944/preprints202408.1495.v1

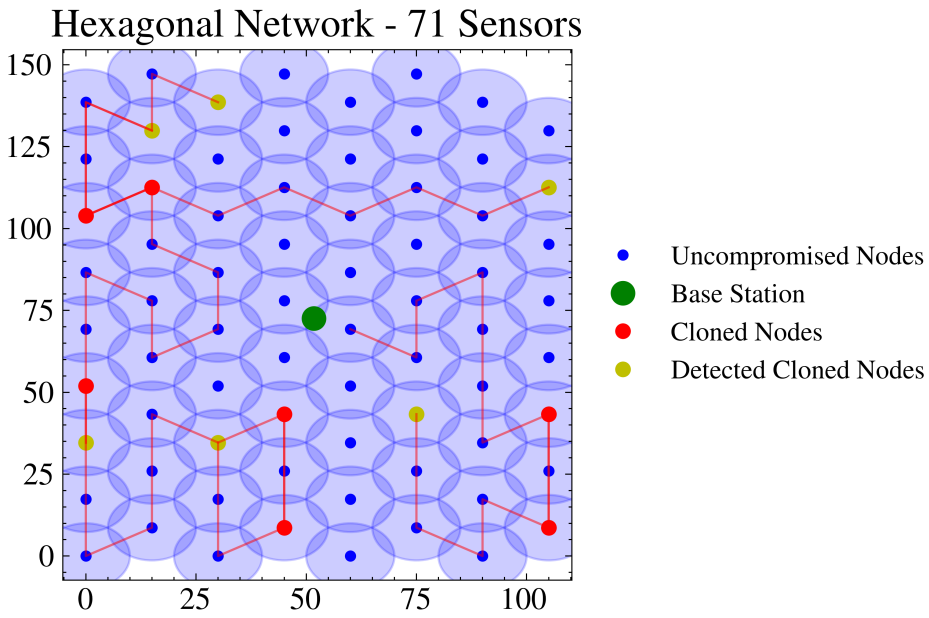

Figure 4. Hexagonal Network.

6.1.4. Triangular Topology

The Triangular topology Figure 5 performs better than the Hexagonal and Square topologies, but not as well as the Aperiodic topology. The dense arrangement of nodes in a triangular grid results in high coverage and multiple overlapping regions, which enhance detection capabilities. Each node in this topology has six neighbors at 60-degree angles, providing a robust network structure that complicates the intruder's path. However, the predictability of the triangular pattern can still be a vulnerability if the intruder is familiar with the layout.

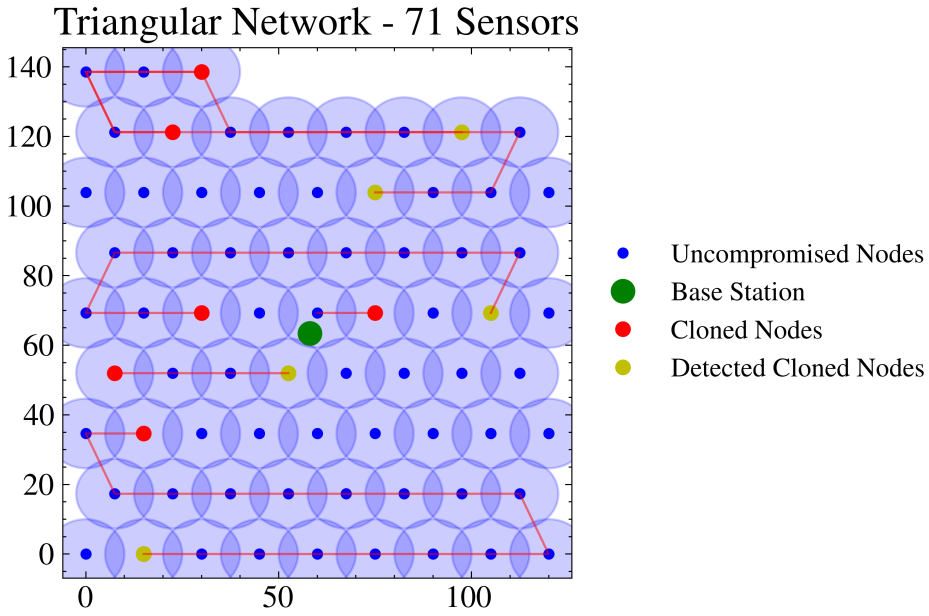

Figure 5. Triangular Network.

6.1.5. Aperiodic Topology

The Aperiodic topology Figure 6, utilizing the Spectre Monotile pattern, shows the lowest base station reached percentage. This indicates a higher resilience against intrusions. The complex and non-repetitive layout creates unpredictable paths, making it difficult for intruders to navigate the

 doi:10.20944/preprints202408.1495.v1

network efficiently. Mathematically, the randomness in sensor placement increases the probability of detection as the intruder cannot easily predict the sensor positions. The high variance in angles and distances between nodes adds to the intruder's difficulty, thereby reducing the likelihood of reaching the base station.

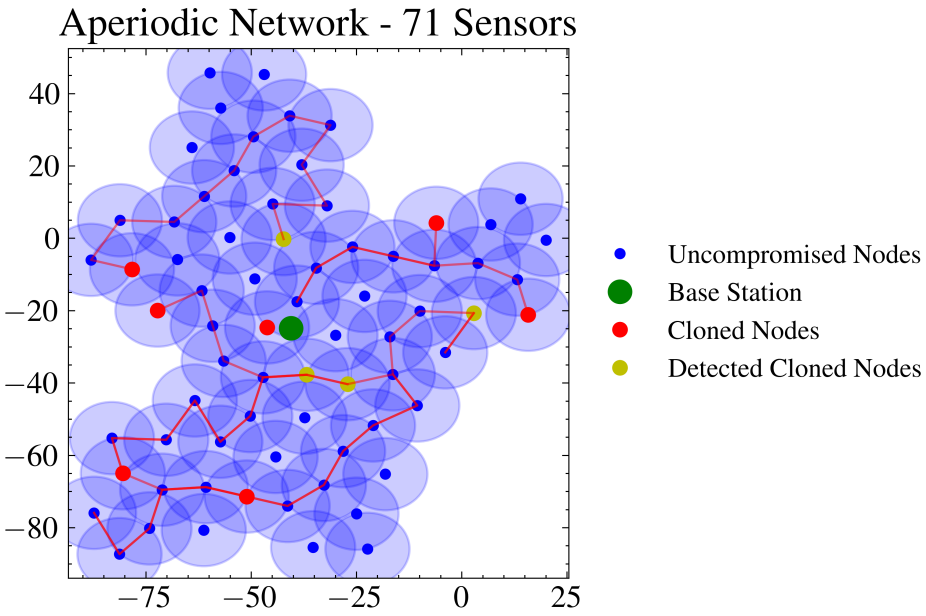

Figure 6. Aperiodic Network.

6.1.6. Graph Interpretation

Figure 7 illustrates the base station reached percentages for each topology. The Aperiodic topology has the lowest percentage, highlighting its superior security due to its complex and unpredictable nature. The Hexagonal and Triangular topologies follow, offering a trade-off between coverage efficiency and security. The Square topology, with the highest percentage, demonstrates the vulnerabilities associated with its predictable layout. The results emphasize the critical role of network topology in enhancing WSN security, with aperiodic tiling providing the best protection against intrusions.

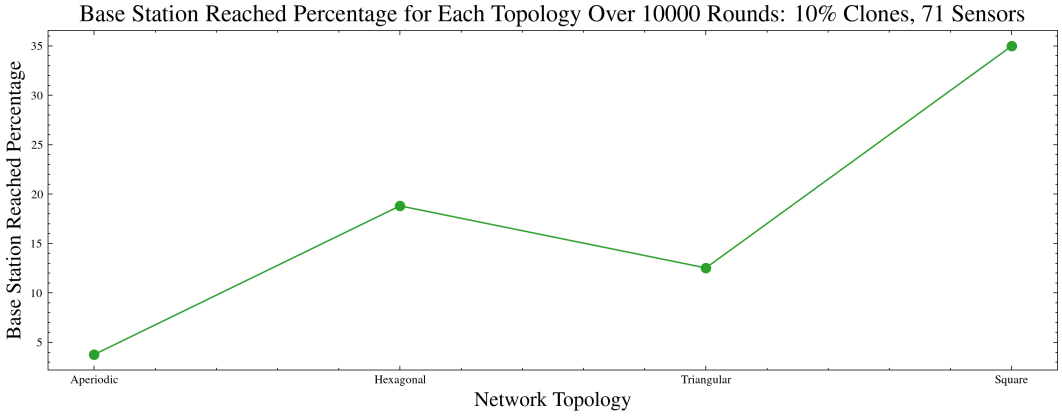

Figure 7. Base Station Reached Percentage for Each Topology.

These findings underscore the importance of considering both the geometric arrangement and the inherent unpredictability of sensor placements when designing secure WSNs. By averaging the results over 10,000 rounds, we ensure that the findings are reliable and reflective of various possible intrusion scenarios, providing a comprehensive assessment of each topology's resilience.

 doi:10.20944/preprints202408.1495.v1

6.2. Total Intrusion Effort

6.2.1. Comparison of Network Resilience

The total intrusion effort required to compromise the network is a comprehensive metric that takes into account the complexity of the network layout, distance traveled by intruders, and size of the network.

6.2.2. Square Topology

The square topology required the least intrusion effort, highlighting its vulnerability due to the regular and straightforward grid pattern.

6.2.3. Hexagonal Topology

The hexagonal topology showed a lower intrusion effort compared to the aperiodic and triangular pattern, but higher than square topology. The predictable yet connected nature of hexagonal grids offers moderate resistance to intruders.

6.2.4. Triangular Topology

The triangular topology demonstrated a higher intrusion effort than the square and hexagonal topology but less than the aperiodic topologies. The unique angles and connectivity in triangular grids enhance network resilience to some extent.

6.2.5. Aperiodic Topology

The aperiodic topology required the highest intrusion effort, reflecting its complex and non-repetitive structure that significantly complicates intruder movement.

Figure 8 presents the total intrusion effort for each network topology. The aperiodic topology exhibits the highest resilience against intrusions, followed by the hexagonal and triangular topologies, while the square topology proves to be the least resilient.

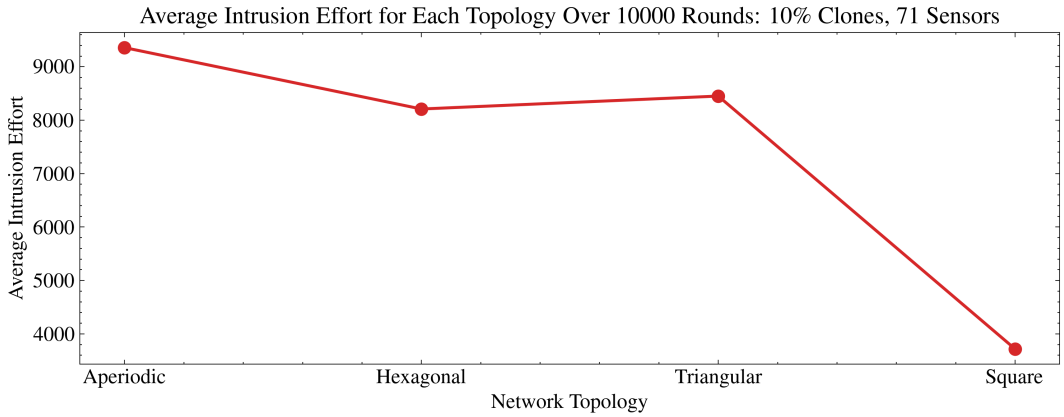

Figure 8. Total Intrusion Effort for Each Topology.

6.3. Average Compromised Nodes

6.3.1. Impact of Redundancy and Coverage

The average number of compromised nodes indicates the extent of network vulnerability to clone attacks. This metric is influenced by the redundancy and coverage provided by each network topology.

6.3.2. Triangular Topology

The triangular topology showed a lower number of compromised nodes than the square topology but higher than the aperiodic and hexagonal topologies. Its unique angles and higher connectivity

 doi:10.20944/preprints202408.1495.v1

improve the network's ability to detect intrusions, but the primary factor is dependent on how far cloned nodes can go before being detected.

6.3.3. Hexagonal Topology

The hexagonal topology had a moderate number of compromised nodes. While it provides good coverage, its regular pattern still allows for some predictability in intruder movement. This is due to it having at most 2-covered regions.

6.3.4. Aperiodic Topology

The aperiodic topology exhibited the second lowest number of compromised nodes. The irregular and complex sensor placement increases the detection probability but more importantly its hotspot regions that are 2,3 or 4-covered allows it to minimize the number of compromised nodes. It is only beat by square topology as that has even higher redundancy.

6.3.5. Square Topology

The square topology exhibited the lowest number of compromised nodes, reflecting its strength in redundancy and multi-redundancy, an idea supported by the barrier coverage papers as well.

Figure 9 shows the average number of compromised nodes for each network topology. The square topology proves to have the lowest compromised nodes, however aperiodic topology comes at second place, and then hexagonal and triangular topology. What must be noted is that the amount of compromised nodes are roughly similar, it is also dependent on the number of times the base station has been reached; as no more nodes are considered to be compromised if the base station is reached. Theoretically, the aperiodic topology should perform better as more malicious cloned nodes are assumed higher in proportion; as it has a good balance between amount of area being covered and multi-coverage.

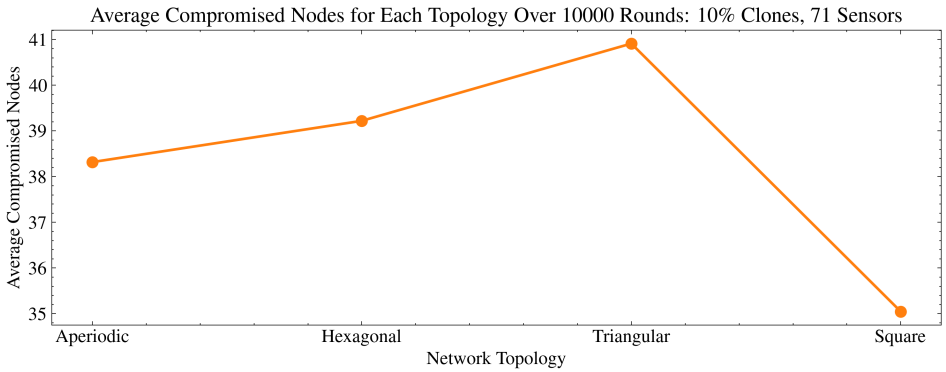

Figure 9. Average Compromised Nodes.

6.4. Average Detections

6.4.1. Detection Efficiency

The average number of detections per simulation run indicates how effectively the network can identify and mitigate intrusion attempts. Detection is directly dependent on hops here, as each hop has a 0 to 10% chance of detection for the cloned node.

6.4.2. Hexagonal Topology

The hexagonal topology showed a moderate number of detections. Its regular pattern provides good area amount coverage, but in terms of detections it still provides a regular pattern, hence not the best detection rate.

 doi:10.20944/preprints202408.1495.v1

6.4.3. Triangular Topology

The triangular topology had the second highest number of detections. Its unique angles and higher connectivity improve detection rates, which is also directly correlated to the intrusion effort graph.

6.4.4. Square Topology

The square topology exhibited the lowest number of detections, indicating its vulnerability and ease of navigation for intruders. This is due to a very simple path to the base station for the malicious nodes.

6.4.5. Aperiodic Topology

The aperiodic topology had the highest average detections. Its complex and unpredictable structure enhances the network's ability to detect intrusions early.

Figure 10 illustrates the average number of detections for each network topology. The aperiodic topology shows the highest detection efficiency, followed by the triangular and hexagonal topologies, with the square topology being the least efficient.

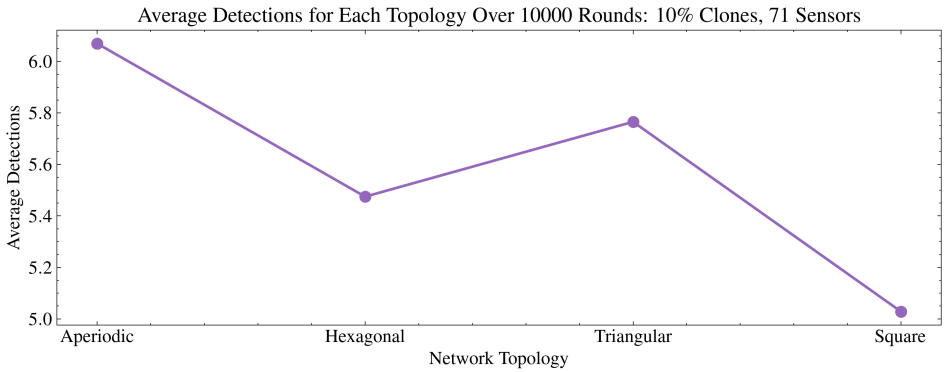

Figure 10. Average Detections.

The average number of hops indicates the efficiency of data transmission within the network. More hops suggest a more complex and less direct communication path.

6.5. Amount of Hops

6.5.1. Square Topology

The square topology exhibited the lowest number of hops, indicating straightforward communication paths that are easier for intruders to exploit.

6.5.2. Hexagonal Topology

The hexagonal topology showed a moderate number of hops. Its regular pattern provides efficient communication paths but is less complex than the aperiodic topology.

6.5.3. Triangular Topology

The triangular topology had a higher number of hops than the square topology but less than the aperiodic and hexagonal topologies. Its unique angles and higher connectivity contribute to a more intricate communication path.

6.5.4. Aperiodic Topology

The aperiodic topology had the highest average number of hops, reflecting its complex structure and the increased difficulty for intruders to navigate the network.n

 doi:10.20944/preprints202408.1495.v1

Figure 11 presents the average number of hops for each network topology. The aperiodic topology demonstrates the most complex communication paths, followed by the hexagonal and triangular topologies, with the square topology having the simplest paths.

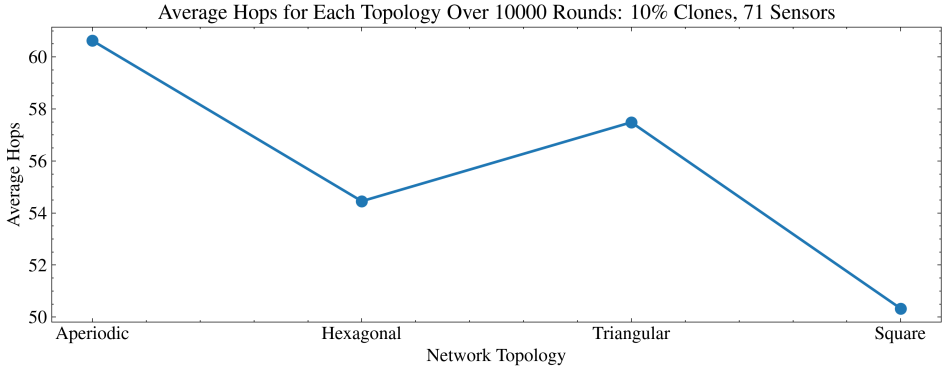

Figure 11. Average Hops.

7. Conclusion

7.1. Summary of Findings

This paper presents an in-depth analysis of the impact of different network topologies on the security of WSNs. Our study introduces the Spectre Monotile aperiodic tiling as a novel approach for sensor deployment, emphasizing its potential to enhance network security. By conducting extensive simulations over 10,000 rounds, we assessed various metrics, including base station reached percentage, total intrusion effort, average compromised nodes, and average detections and hops, across aperiodic, hexagonal, triangular, and square topologies.

For instance, the aperiodic topology superiority has been highlighted by comparison throughout the paper. The aperiodic tiling demonstrated the lowest base station reached percentage, highest intrusion effort, and lowest number of compromised nodes, highlighting its superior resilience against intrusions due to its complex and unpredictable layout.

Moreover, periodic topology were shown to have weak or little security. For example, hexagonal and triangular topologies showed moderate resilience, benefiting from their unique angle. This provided a somewhat balance between coverage and security. Hexagonal grids offered good coverage but were more predictable than aperiodic patterns, while triangular grids had high coverage density with unique angles aiding detection. Even more so, square topologies exhibited the highest base station reached percentage and the lowest intrusion effort. Clearly, indicating its vulnerability due to its simple and predictable layout. Although, high redundancy, the ease of navigation for intruders reduced its overall security.

Finally, the effectiveness of IEI was proved to be a valuable metric for quantifying the effort required for intruders to navigate through the network. By incorporating distance, network complexity, and detection capabilities, IEI provided a comprehensive measure of network resilience.

7.2. Contributions to the Field

This research makes significant contributions to the field of WSN security. The application of the Spectre Monotile aperiodic tiling for sensor deployment in WSNs is a novel approach that enhances security through its non-repetitive and complex structure. Moreover, we have developed the IEI Metric offering a robust framework for evaluating and comparing the security of different network topologies, integrating structural properties with traditional security measures. Lastly, our simulation analysis has provided practical insights into the performance of various network topologies, guiding the design and deployment of more secure WSNs.

 doi:10.20944/preprints202408.1495.v1

7.3. Future Work

While these results are noteworthy, they leave some avenues open for further exploration and improvement:

Further investigation into other aperiodic tiling patterns and their impact on WSN security by considering heterogeneous sensor networks (using more than one tile) could provide additional insights and potential improvements. This leads to the potential of hybrid topologies that combine periodic and aperiodic tiling patterns. By leveraging the strengths of both approaches, it would optimize both coverage and security. Additionally, developing mechanisms for dynamically adapting network topology using mobile sensors to form an aperiodic arrangement could enhance resilience and recovery in real-time. This approach could allow the network to self-organize in response to detected intrusions or changing environmental conditions.

Moreover, the sensor density for achieving at least 1-coverage in aperiodic spectre tiling is 0.006, which is better than triangular and square topologies but worse than hexagonal grids. However, aperiodic tiling has regions that are 2, 3, or even 4-covered, unlike hexagons, which only have 2-covered regions. Proper utilization of this redundancy could make aperiodic tiling more feasible and practical. This adaptability makes aperiodic spectre monotiling potentially more suitable for real-life deployment scenarios, as the irregular regions formed by aperiodic spectre monotiling might provide more effective coverage in diverse and unpredictable environments.

The high fault tolerance and redundant coverage of aperiodic spectre tiling make it a promising candidate for applications where network partitioning and robustness are critical. Further research could explore these properties in greater detail to enhance network resilience. Combining the benefits of aperiodic tiling with advanced intrusion detection and response protocols could further strengthen the overall security framework of WSNs. This integration would provide a holistic approach to securing WSNs against various types of attacks.

Balancing the improved security with energy efficiency remains a critical challenge. Future work should focus on optimizing sensor placement and network operations to maintain long-term viability while minimizing energy consumption. In this regard, future studies should explore the eight distinct clusters Γ (Gamma), Δ (Delta), Θ (Theta), Λ (Lambda), Ξ (Xi), Π (Pi), Σ (Sigma), and Φ (Phi) which allow for spectre's aperiodic tiling. The exploration of these clusters may provide insights into improving security and energy efficiency.

Given that spectre originates from common hexagonal tiling, integrating a 'sub-layering' method could enhance security. This method would exploit the connection between spectre and hexagonal tiling to transform compromised network topologies into secure aperiodic tessellations. Finally, leveraging mobile sensors to convert random topologies into aperiodic networks could establish security in dynamic and potentially hazardous environments.

This paper has explored the practical uses of aperiodic tiling and established coverage and connectivity, which is essential for sensor deployment. Building off on this, we have developed a quantifiable metric to measure the spatial complexity of network topologies during cloned node attacks, and constructed a robust framework to simulate selective forwarding intrusion methods as well. From our experiments, we have discovered that the non-periodic pattern enhances the security of WSNs and is a feasible and practical approach for implementation in real-world scenarios.

Acknowledgments: We would like to express our heartfelt gratitude to the individuals at Texas A&M University-Kingsville, who have supported our research opportunity for undergraduates program. First and foremost, we thank our sole principle investigator Dr. Ammari, for his guidance, expertise, and continuous encouragement throughout the entire program. His ever-growing knowledge of WSNs have been instrumental in shaping this work. Special thanks go to the department of Electrical Engineering and Computer Science for providing access to essential resources to run computational intensive simulations. We would also like to acknowledge the financial support provided by National Science Foundation. The funding allows our fellow colleagues and ourselves to financially be sound of mind.Lastly, we extend our appreciations to the fellow colleagues in the cohort and the broader Texas A&M - Kingsville community for creating a nurturing and supportive academic environment.

 doi:10.20944/preprints202408.1495.v1

References

1. H. M. Ammari, "Achieving Sensing k-Coverage Using Hexagonal Tiling: Are We Done Yet?" in *2019 IEEE 16th International Conference on Mobile Ad Hoc and Sensor Systems (MASS)*, 2019, pp. 73-81, doi: 10.1109/MASS.2019.00018.
2. D. Smith, J. S. Myers, C. S. Kaplan, and C. Goodman-Strauss, "A chiral aperiodic monotile," 2023. [Online]. Available: https://arxiv.org/abs/2305.17743.
3. P. A. Birjandi, L. Kulik, and E. Tanin, "K-coverage in regular deterministic sensor deployments," in *2013 IEEE Eighth International Conference on Intelligent Sensors, Sensor Networks and Information Processing*, 2013, pp. 521-526, doi: 10.1109/ISSNIP.2013.6529844.
4. Z. Chen, M. Jia, Y. Wang, and X. Yan, "A Security Topology Protocol of Wireless Sensor Networks Based on Community Detection and Energy Aware," in *2015 IEEE Trustcom/BigDataSE/ISPA*, 2015, pp. 1284-1289, doi: 10.1109/Trustcom.2015.519.
5. L. K. Bysani and A. K. Turuk, "A Survey on Selective Forwarding Attack in Wireless Sensor Networks," in *International Conference on Electronics and Information Engineering*, 2011, pp. V1-260-V1-264, doi: 10.1109/ICEIE.2010.5559821.
6. M. Keerthika and D. Shanmugapriya, "Wireless Sensor Networks: Active and Passive attacks - Vulnerabilities and Countermeasures," *Global Transitions Proceedings*, vol. 2, no. 2, pp. 362-367, 2021, doi: https://doi.org/10.1016/j.gltp.2021.08.045.
7. I. Butun, S. D. Morgera, and R. Sankar, "A Survey of Intrusion Detection Systems in Wireless Sensor Networks," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 1, pp. 266-282, 2014, doi: 10.1109/SURV.2013.050113.00191.
8. Y. Zeng, J. Cao, S. Zhang, S. Guo, and L. Xie, "Random-walk based approach to detect clone attacks in wireless sensor networks," *IEEE Journal on Selected Areas in Communications*, vol. 28, no. 5, pp. 677-691, 2010, doi: 10.1109/JSAC.2010.100606.
9. B. Liu, O. Dousse, J. Wang, and A. Saipulla, "Strong barrier coverage of wireless sensor networks," in *Proceedings of the 9th ACM International Symposium on Mobile Ad Hoc Networking and Computing*, New York, NY, USA: Association for Computing Machinery, 2008, pp. 411–420, doi: 10.1145/1374618.1374673.
10. S. Luo, Y. Lai, and J. Liu, "Selective forwarding attack detection and network recovery mechanism based on cloud-edge cooperation in software-defined wireless sensor network," *Computers & Security*, vol. 126, p. 103083, 2023, doi: https://doi.org/10.1016/j.cose.2022.103083.
11. F. Shahzad, M. Pasha, and A. Ahmad, "A Survey of Active Attacks on Wireless Sensor Networks and their Countermeasures," *International Journal of Computer Science and Information Security (IJCSIS)*, vol. 14, no. 12, pp. 54-65, Dec. 2016.
12. M. Y. Aalsalem, W. Z. Khan, and N. M. Saad, "Detecting clones in wireless sensor networks using constrained random walk," in *2015 International Conference on Radar, Antenna, Microwave, Electronics and Telecommunications (ICRAMET)*, 2015, pp. 55-59, doi: 10.1109/ICRAMET.2015.7380774.
13. S. Kumar, T. H. Lai, and A. Arora, "Barrier coverage with wireless sensors," in *Proceedings of the 11th Annual International Conference on Mobile Computing and Networking*, 2005, pp. 284-298, doi: 10.1145/1080829.1080859.
14. V. Gharavian, R. Khosrowshahli, Q. H. Mahmoud, M. Makrehchi, and S. Rahnamayan, "Intrusion Detection for Wireless Sensor Network Using Graph Neural Networks," in *2023 IEEE Symposium Series on Computational Intelligence (SSCI)*, 2023, pp. 807-813, doi: 10.1109/SSCI52147.2023.10372004.
15. A. Diaz and P. Sanchez, "Simulation of Attacks for Security in Wireless Sensor Network," *Sensors*, vol. 16, no. 11, article 1932, 2016. Available: https://www.mdpi.com/1424-8220/16/11/1932.

Short Biography of Author

Ayaz Khan is a senior at Hunter College, majoring in Statistics, with a passion for data science, analysis and encryption. His interests include data, applied mathematics and information synthesis. He hopes to pursue a Ph.D in Data Science and learn more about Quantum Cryptography alongside. Moreover, he also has a passion towards political science from time to time as an avid vocalist of justice and human rights.

Gabriel Macias-Villegas is a sophomore at the University of Nebraska - Lincoln for a B.S in Electrical Engineer and a B.S in Mathematics. The research opportunity for undergrads program has given him ambitions to purse

 doi:10.20944/preprints202408.1495.v1

at least a M.S in Electrical Engineer if not a Ph.D. in the near future. In all cases, he believes that learning is continuous string of adventures that doesn't stop in education but, extends to life.

Habib M. Ammari is a Tenured Full Professor and the Founding Director of the Wireless Sensor and Mobile Autonomous Networks (WiSeMAN) Research Lab at Texas A&M University-Kingsville (TAMUK). He joined TAMUK in 2019 and has received multiple Professor of the Year awards, as well as the Outstanding Graduate Instructor Teaching Award. He previously served as the Graduate Computer Science Program Director at TAMUK and has held tenured positions at the University of Michigan-Dearborn and Sup'Com Tunis, Tunisia. Dr. Ammari earned two Ph.D. degrees in Computer Science, with research interests in wireless sensor networks, network security, and computational geometry. He has a strong publication record in top-tier journals and conferences and has authored several Springer books on wireless sensor networks. Dr. Ammari is the recipient of the NSF CAREER Award and numerous other prestigious accolades. He is an IEEE Senior Member and has served as an Associate Editor for several leading journals, in addition to his extensive service in organizing and chairing international conferences.