On Protecting a Vulnerable Area in Mobile Sensor Networks

Kuei-Ping Shih, Chun-Chih Li, Chien-Hua Cheng, and Shen-Rong Lin

Department of Computer Science and Information Engineering
Tamkang University, Tamshui 251, Taipei, Taiwan
Email: kpshih@mail.tku.edu.tw

摘要

本篇論文探討在無線感測網路中,假使存在一重要區域，如何使網路中的重要的區域不成為 Sensor Nodes 感測能力最薄弱路徑的一部分，進而達到防禦的目的。本論文提出一個藉由 Sensor Nodes 的移動來改變網路上入侵者入侵的路徑，使入侵之路徑，不會經過網路上的重要區域。同時，為了避免消耗過多的 Sensor Nodes 的電量，本篇論文所提出的演算法只需移動少數的 Sensor Nodes，即可改變網路上受到 Sensor Nodes 感測能力最薄弱的路徑。實驗結果顯示出，本論文所提出的方法可以使 Sensor Nodes 以較少的電量移動，同時使網路中受到 Sensor Nodes 感測能力最薄弱的路徑不再經過重要區域。

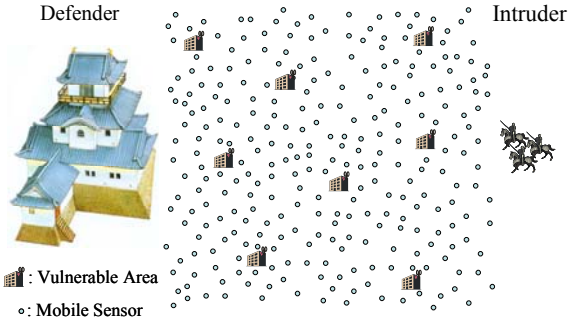
關鍵詞：Wireless Sensor Networks、Mobile Sensor、Voronoi Diagram、Vulnerable Area、Coverage

1. 簡介

隨著無線通訊技術的發展，使得體積小、低成本、多功能的無線感測器(Sensor Nodes)大量被應用在生活上。Wireless Sensor Networks 可以廣泛應用於各種場景中，例如：戰場上的軍事偵測、自然保育區的生態監控、自然災害的警報、災區的探測與監視等各種不同的環境中，或是在健康醫療和家庭上的應用。

本論文試考慮以下場景：假設戰場上左方有一 Defender，如圖一所示在這 Defender 的外面有數個對外的通訊站，這些通訊站是作為與對外聯繫的通訊基地，因此通訊站視為很重要的區域。假設在這許多的通訊站周圍佈建許多 Sensor Nodes，藉以感測通訊站周遭環境的情形，然而 Sensor Nodes 電量皆為有限，因此隨著網路時間的增加，而產生電量耗盡或是故障損壞，使網路上產生空洞區(Coverage Holes)。

此時若有入侵者欲攻擊左方的 Defender 時，則此入侵者必須經過 Defender 前方佈建 Sensor Nodes 的區域，如圖一所示。此入侵者如欲入侵此區域，必定會希望穿越網路中感測能力較薄弱的區域。故當此通訊站位於網路中感測能力較薄弱的區域時,則入侵者可能會穿越 Wireless Sensor Networks，到達通訊站周圍，並加以破壞，使得



圖一. 場景圖

Sensor Nodes 監控環境的作用喪失。因此，若使用具有移動裝置的 Sensor Nodes，則可以利用 Sensor Nodes 的移動，改善通訊站附近的感測能力，使入侵者入侵此區域時，不會再經過任一個通訊站，而能達到保護通訊站的目的。

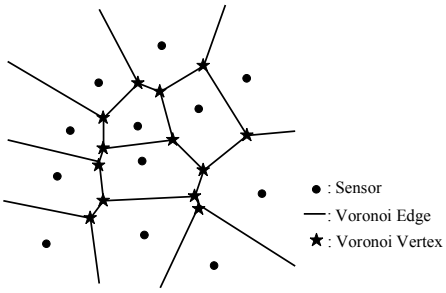
由於 Sensor Nodes 的能量來源通常為電池，因此各種在 Wireless Sensor Networks 上的演算法大部分會以電量考量為優先。為了使 Sensor Nodes 能有效的節省電量的消耗,並且能使 Sensor Nodes 移動過後，網路上受到 Sensor Nodes 感測較薄弱的區域能遠離通訊站。本篇論文將利用具移動能力的 Sensor Nodes 來協助改善易感測能力薄弱之路徑，並希望所提出的演算法能夠使移動的 Sensor Nodes 數量最少且 Sensor Nodes 移動的總距離最少，以達到減少 Sensor Nodes 的耗電量，並進而延長網路 Lifetime。

本論文後續章節的架構如下:第 2 章將概述本論文所使用到的背景知識與相關研究，第 3 章則為本篇論文所提出的演算法，第 4 章為實驗結果，第 5 章則針對這篇論文做結論。

2. 背景知識與相關研究

2.1. 背景知識

當入侵者入侵時，根據 Sensor Nodes 的 Detection Probability Model，Sensor Nodes 的感測能力會隨著距離的增加而減少。因此，入侵者其行走的方式便會往距離任兩個 Sensor Nodes 間最遠的距離行進，因此，藉由對任兩個 Sensor Nodes 作中垂線可分析出每個 Sensor Nodes 涵蓋的 Coverage，此一圖形又稱為 Voronoi Diagram[1]。



圖二. Voronoi Diagram

在圖二中，圓形圖示即為 Sensor Nodes，黑色的線段代表 Voronoi Edge，每個 Voronoi Edge 相交的頂點稱為 Voronoi Vertex，星形圖示即是。在一個 Voronoi Cell 區域裡的任一位置，皆只會與一個 Sensor Nodes 最靠近，Voronoi Edge 即為受到任兩相鄰的 Sensor Nodes 感測機率最為薄弱的區域，因此所有的 Voronoi Edge 就是代表網路上最不易受到 Sensor Nodes 感測的區域。

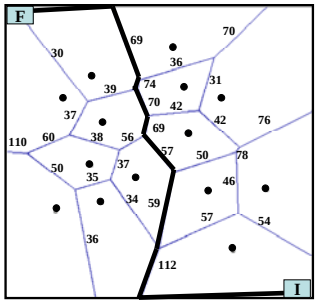
本論文將以 Voronoi Diagram 分析佈建於網路上 Sensor Nodes 其 Coverage 的情形，論文中將每個 Voronoi Edge 及與 Voronoi Edge 具有最短距離的 Sensor Nodes 之距離給予 Weight 值，如圖三所示，即 Sensor Nodes 至 Voronoi Edge 的垂直距離，Weight 值越大，代表 Voronoi Edge 受到 Sensor Nodes 感測的機率越低，Weight 值越小，代表 Voronoi Edge 受到 Sensor Nodes 感測的機率越高。

2.2. 相關研究

如何找出網路上受到 Sensor Nodes 感測能力最為薄弱的區域目前已有相關文獻[2][4][6]進行討論，並被定義為 Worst-Case Coverage Problem。在這樣的環境中，就會存在一條最容易被入侵者入侵的路徑，稱為 Maximal Breach Path。這樣的一條路徑會與網路上的 Sensor Nodes 有最大的距離，如圖三所示。在[2] [4] [5]的研究中，皆是利用所找出的 Maximal Breach Path，額外的增加 Sensor Nodes 至網路上感測品質最為薄弱的區域。

研究[4]考慮在全為 Static Sensor Nodes 的網路上，如何找出網路上感測能力最薄弱的區域。研究[4]利用目前網路上 Sensor Nodes 的 Topology 來形成一 Voronoi Diagram，並利用此 Voronoi Diagram 找出一條網路上受到感測能力最薄弱的路徑，稱之為 Maximal Breach Path。

此篇論文採用集中式的方式，先找出 Voronoi Edge 上 Weight 值最大和最小者取中間值，此中間值即為所設定的 Threshold 值。其演算法採用的是 Binary Search 的方式，若大於目前 Threshold 值的 Voronoi Edge 能形成一條路徑穿越網路兩端時，則再將此 Threshold 值提高；反之，若無法形成一條路徑穿越網路兩端時，則將此 Threshold 值降低，重複此步驟直到找出最佳的 Threshold



圖三. Maximal Breach Path [4]

值，稱此 Threshold 值為 Breach Value，而所找出的路徑即為 Maximal Breach Path，且此演算法只需在 Polynomial Time 內即可完成。

研究[5]是在已佈建好的網路中，藉由額外的增加 Sensor Nodes 來改善目前網路上的 Coverage。此篇論文是以 Path-Based 的方式找尋網路上感測能力薄弱的區域，找出侵入者最容易穿越網路的一條路徑，並以 Exposure Value [3]來代表網路上受到 Sensor Nodes 感測能力的程度。作者提出了四種不同的方法選擇增加的 Sensor Nodes 需放置的位置，以達到改善目前網路上的 Coverage。

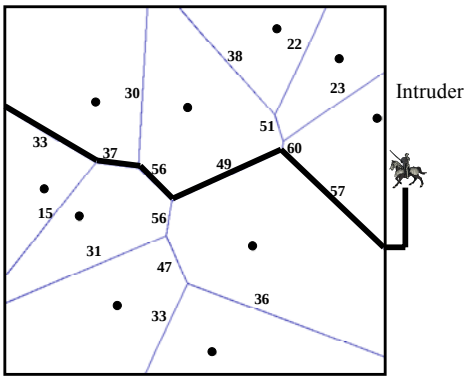
3. 重要區域保護機制-VAPM

本論文將提出的保護重要區域的方法，稱為 Vulnerable Area Protection Movement Protocol (VAPM)。VAPM 首先找出入侵者會進入到重要區域的路徑，利用 Sensor Nodes 的移動改變，以避免重要區域成為入侵者入侵路徑上的區域，因此，當入侵者入侵的路徑不經過重要區域時，則不需進行此演算法。

3.1. 網路環境

本篇論文假設場景為在一廣大的區域中，入侵者想橫越此區域。在本篇論文中，為了簡化問題，將此一廣大區域分為許多的區塊，在每一網路區塊裡，皆只會有一個重要區域。在本論文所提出的方法中，主要是針對一個被分割的小區域進行。當網路上每一個小區域，若都能滿足不通過重要區域的條件，則整個網路的重要區域都不會被穿越。

入侵者進入 Sensor Nodes 的區域時，因為入侵者希望沿著一條會沿著 Voronoi Edge 行走，根據自己目前所在的位置與鄰近的 Sensor Nodes 的位置資訊，而選擇一受到 Sensor Nodes 感測能力最為薄弱的路徑行進，如圖四所示，入侵者有 Weight 值為 23 和 57 路徑可以選擇。在本篇論文中入侵者會選擇 Weight 數值為 57 的 Voronoi Edge 前進。之後，皆根據此原則判斷前進的方向。接下來可以選擇的路徑有 Weight 值為 60 和 49 的 Voronoi Edge。此時，雖然 Weight 值是 60 的 Voronou Edge 是入侵者較佳的選擇，但由於



圖四. 入侵者入侵路徑選擇

Weight 值是 60 的 Voronou Edge 方向是往回走的，因此此一 Voronou Edge 並不會被選擇，入侵者會選擇 Weight 值為 49 的 Voronoi Edge 前進。

3.2. Vulnerable Area Protection

當入侵者入侵的路徑經過重要區域時，要移動某些 Sensor Nodes 避免入侵者的路徑經過重要區域。此時，最直覺的方式便是直接將 Sensor Nodes 移動到重要區域的附近，使重要區域的附近受到 Sensor Nodes 的感測機會增加，使入侵者入侵的路徑不再經過重要的區域。然而，這樣的作法可能造成以下的缺點:

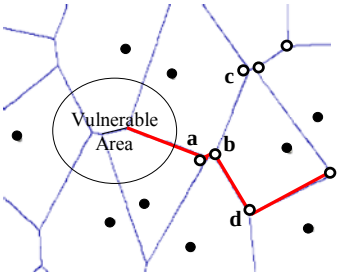
(一) 所移動的 Sensor Nodes 需移動較多的距離，而造成消耗較多的電量。

(二) Sensor Nodes 移動過後的路徑仍然會再經過重要區域，無法使入侵的路徑不經過重要區域，使成重要區域仍遭到入侵者入侵。

本論文將對所提出的 VAPM 分為四個部份進行介紹，第一個部份為 Critical Vertex Searching，其主要目的是找出所有會進入到重要區域的 Voronoi Edge 其相鄰的 Voronoi Vertices。進而找出能使入侵者入侵的路徑能轉向，且不會再進入重要區域的 Critical Vertices。第二部份為 Critical Vertices Moving，將討論要如何移動 Sensor Nodes，才能改變入侵者移動的路徑，並計算出所需要移動的距離。由於在第二個找出來移動的點可能有相當多可能性。因此，第三個部份將探討 Critical Sets Selection，目的為找出多組的 Critical Sets，每一組的 Critical Sets 都代表一種可能移動的情形。第四個部份為找出 Optimal Critical Set，根據 Sensor Nodes 的剩餘電量找出花費最少電量的 Critical Set。以下將詳述這四個部份的作法和細節。

3.2.1 Critical Vertices Searching

這個 Phase 主要目的是找出所有 Critical Vertices。Critical Vertices 的意義即是當入侵者走到位於圖形上得這些 Voronoi Vertices 時，則接下來入侵者的路徑一定會進入到重要區域。



圖五. Critical Vertices Searching

為了要找出會導致入侵者路徑經過重要區域的 Voronoi Vertices，本論文使用回溯追蹤為找尋 Critical Vertices 的策略，意即從重要區域往回找尋所有會導致入侵者路徑進入到重要區域的 Voronoi Vertices。因此在尋找 Critical Vertices 的方法上，首先考慮會經過重要區域的 Voronoi Edges，接著從這些 Voronoi Edges 的進入端點 Voronoi Vertices 開始進行判斷。若會經過重要區域的 Voronoi Edge 是所有入侵者在此一 Voronoi Vertex 可能行走的路徑中 Weight 值最大的，則表示若當入侵者的路徑行走到此一 Voronoi Vertex 時，必定會選擇該條會經過重要區域的 Voronoi Edge 行走，因此這樣的 Voronoi Vertex 即稱為 Critical Vertex。當成為 Critical Vertex 時，及表示此一 Voronoi Vertex 會使入侵者的路徑進入到重要區域，因此會使入侵者走到此一 Critical Vertex，也應為 Critical Vertex。所以，當一個點成為 Critical Vertex 時，必須往前判斷其他的 Critical Vertices 會不會走到這一個 Critical Vertex，進而走到重要區域。

如圖五所示，一開始以連結重要區域之端點 *a* 開始判斷是否為 Critical Vertex。在 Voronoi Vertex *a* 上，發現進入重要區域之 Voronoi Edges 為 Voronoi Vertex 中所有向外連結之 Voronoi Edges 中 Weight 值最大之邊。則表示入侵者在 Voronoi Vertex *a* 判斷時，會進入重要區域。此時，Voronoi Vertex *a* 應被判斷為 Critical Vertex，且必須對進入到 Voronoi Vertex *a* 的 Voronoi Vertex *b* 進行判斷其是否為 Critical Vertices。在 Voronoi Vertex *b* 上，其最大 Weight 值的 Voronoi Edges 會連結到 Critical Vertex，表示當入侵者到達 Voronoi Vertex *b* 時，會進入 Voronoi Vertex *a* 然後進入重要區域，因此 Voronoi Vertex *b* 也會被判斷為 Critical Vertex，並對連結至 Voronoi Vertex *b* 的 Voronoi Vertex *c* 跟 Voronoi Vertex *d* 進行判斷是否為 Critical Vertex。同理，此一方法可以拓展至整個網路。

3.2.3 Critical Sets Selection

在 3.2.1 中找出在網路中的 Critical Vertices 會影響入侵者的路徑。然而，Critical Vertices 只決定網

路中會影響入侵者的路徑的 Voronoi Vertex，尚些 Critical Vertices 使路徑產生改變。在本小節中將討論移動哪一些 Sensor Nodes 可以使路徑產生改變。首先，若要改變入侵者入侵的路徑，則必須選一個在路徑上的 Voronoi Vertex 進行改變，如此才能使入侵的路徑改變。然而，只改變路徑上的點是不夠的，若單是改變在路徑上 Voronoi Vertex，則改變完之後之後，仍有可能會連結到 Critical Vertices。此時，雖然改變了路徑，但是仍然會進入重要區域。因此，當改變的路徑上的 Critical Vertices 之後的路徑若是仍是連結到 Critical Vertices，則必須在挑其他的點形成一組 Critical Set，使得重複進入的問題不會發生。

考慮上面所提到之問題，因此本論文中將所找出的 Critical Vertices 分成安全的 Critical Vertices 和危險的 Critical Vertices。安全的 Critical Vertices 即為 Critical Vertices 中，和不為 Critical Vertex 的 Voronoi Vertex 相鄰，表示如果轉動這個 Voronoi Vertex 即可將入侵者的路徑轉動到不會進入重要區域的路徑上。剩餘的 Critical Vertices 因為無論改變路徑到任一條路徑上都會遇到 Critical Vertices，進而再次進入到重要區域，這些 Critical Vertices 即為危險的 Critical Vertices。

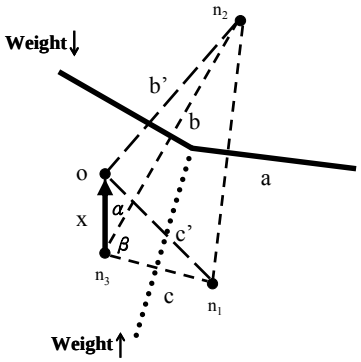
首先，從原本入侵者入侵的路徑上開始找起，在路徑上的每一個 Critical Vertices 即為一種 Critical Set。然而，若是在路徑上形成的 Critical Sets 中僅包含一個危險的 Critical Vertex，則必須找出另外一個安全的 Critical Vertices 與之搭配，形成一個 Critical Set；反言之，在路徑上安全的 Critical Vertex 即可單獨形成一個 Critical Sets。藉由這樣的組合產生多組 Critical Sets，每一組的 Critical Set 都可以使入侵者的路徑產生改變。

3.2.2 Critical Vertices Moving

藉由前面所提到的回溯追蹤的策略，可以找出 Critical Vertex。然而，仍必須藉由移動 Sensor Nodes 以改變 Critical Vertices，才能使原先入侵者入侵的路徑改變。因此，在本小節中將要去考慮要如何移動 Sensor Nodes，使入侵者入侵的路徑改變。在本論文中，將提出為三個不同的移動策略，以下將敘述三個移動策略:

改變 Weight 值

第一個提出的移動策略即為改變路徑的 Weight 值，進而改變入侵者在 Critical Vertex 所作的判斷。如圖六所示，假設入侵者入侵的路徑為行經 Edge *a* 後再經過 Edge *b*，表示目前網路上 Edge *b* 的 Weight 值大於 Edge *c* 的 Weight 值，然而由於走往 Edge *b* 的路徑會通往重要區域，因此我們需將 Edge *b* 和 Edge *c* 的 Weight 值分別做改變，使 Edge *b* 的 Weight 值小於 Edge *c* 的 Weight 值，而使原本的入侵者改為經由 Edge *c* 路徑前進，將不再通往重要區域。



圖六. 同時改變兩相鄰 Voronoi Edge 的 Weight 值

在本論文中希望移動最少的 Sensor Nodes，然而，要移動最少的 Sensor Nodes 數目，最好能移動同時能影響兩邊 Voronoi Edge 的 Weight 值。因此，最好的方式是移動形成兩 Edge 的共同 Sensor Nodes n_3。

如圖六所示，假設改變兩個 Edge 的 Weight 值最佳的位置在 *o* 點。要移動到 *o* 點，需要將 Sensor Nodes n_3 朝 α 角移動 *x* 距離，α 角為移動的方向與 Edge *b* 鉛垂線之夾角，β 角為原來 b 與 c 之夾角，*b'*與 *c'*為在 Sensor Nodes n_3 移動後，新的 Weight 值。

在提出的方法中，欲交換 *b* 和 *c* 的 Weight 值。使 *c'*大於 *b'*。因此可得移動距離與移動角度間關係，如下式

$$x = \frac{b^2 - c^2}{2b\cos\ \alpha - 2c\cos(\ \alpha + \beta)} \qquad (1)$$

透過上式，可計算出移動 *x* 距離後，可以使路徑改變。然而在上式中，移動的角度 α 仍是未知數。此時考慮改變 Weight 值時，使所移動 Sensor Node 移動距離為最小，因此透過解此微分方程。可得當移動的角度為下面所計算出之 α 角時，可以使所移動的距離 *x* 最小

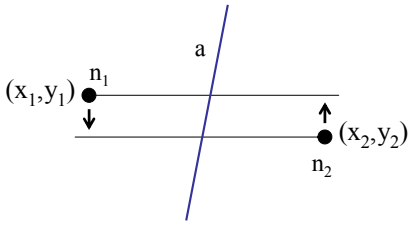
$$\alpha\ =\ \tan^{-1}(\frac{\text{csin}(\ \ \beta\ )}{\text{b - ccos}(\ \ \beta\ )}) \qquad (2)$$

在求得 α 的角度後，由於 β 為已知，因此將 α 和 β 帶入原式中，即可以求出所需移動的距離。

改變路徑斜率

在本論文中，假設入侵者只會往前行進，不會有往回走的情形。因此在本方法中，將利用此一特性，改變入侵者所走的 Voronoi Edge 的斜率，進而使入侵者改變行走的路徑。

如圖七所示，此 Voronoi Edge *a* 的斜率為正值，若要使此 Voronoi Edge 的斜率成為負值，則可移動 Sensor Node n_1 或 n_2，兩 Sensor Nodes 的座標分別為(x_1,y_1)和(x_2,y_2)，若移動 Sensor Node n_1，則需往垂直向下的方向移動，若移動 Sensor Node n_2，則需往垂直向上的方向移動，而改變 Voronoi Edge 的斜率所需移動的距離為$|x_1-x_2|+s$，*s* 為任何大於 0 的常數。



圖七. 改變 Voronoi Edge 斜率

路徑消除

當 Voronoi Diagram 形成一極短的 Voronoi Edge 時，則只需移動少許距離即可使此 Voronoi Edge 消失，並使其原相鄰的 Edge 交於一點。這樣的移動法則為一特例的情形。

如圖八所示，假設入侵者入侵的路徑為行經 Edge *a* 後再經過 Edge *b* 和 Edge *c*。然而，Edge *b* 為一極短的 Voronoi Edge，若要使 Edge *b* 消失，則 Sensor Nodes 只需移動少許的距離。由於目前網路上的 Edge *c* 的 Weight 值小於 Edge *d* 的 Weight 值，表示若能將 Edge *b* 消除，使 Edge *c* 和 Edge *d* 相交於一點，則使入侵者入侵的路徑變成通往 Edge *d*，即不再通往重要區域。因此，在本節中將提出使 Voronoi Edge 消失的方式，使入侵者入侵的路徑不再進入重要的區域。

3.2.4 Optimal Critical Set

在 3.2.3 中找出多組可以改變入侵者路徑的 Critical Sets。然而，在本篇論文中，不僅希望能找出一組使入侵者路徑改變的解，更希望考慮到 Wireless Sensor Networks 的特性，減少耗電。因此，在本小節中，將討論如何從多組的 Critical Sets 中，找出移動所需花費最少 Cost 的 Critical Set。

一個 Mobile Sensor 移動的電量，可分為一開始所需要克服靜磨擦需要的電量，以及移動時每單位距離的耗電。因此，在本論文中，將 Mobile Sensor 的移動所需要的耗電表示下列式子

$$E_c = \delta + d * \Delta m$$

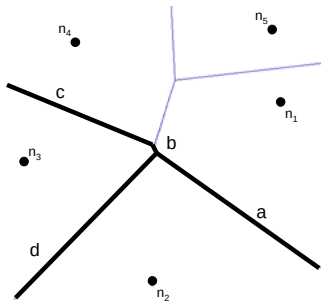
E_c 表示移動所需耗費的電量，δ 表示 Mobile Sensor Nodes 從靜止到移動狀態時所需耗費的初始電量，d 表示移動的距離，Δm 表示 Sensor Nodes 每移動一單位所需耗費電量大小。

根據電量消耗的公式，可以將 3.2.3 找出來的 Critical Sets，計算出每一組 Critical Sets 改變路徑時所需要的電量。從所有的 Critical Sets 中，找出一組所需要之移動電量為最少的 Critical Sets，即為本論文認為之最佳解。

4.實驗

4.1 實驗環境及參數

本論文利用 C++ 撰寫模擬程式來評估本論文所提出之演算法。本論文實驗場景為在 500m×500m 的網路環境下，隨機佈建 150 個



圖八. 消除 Voronoi Edge

Sensor Nodes，並採用 50 次不同的網路佈點情形，分別模擬本篇論文採用之方法以及比較方法，比較其消耗之電量。為了能評估 Sensor Nodes 移動後消耗的總電量，本論文引用前面所定義之電量消耗公式。其中 Sensor Nodes 從靜止到移動狀態時所需耗費的電量為 2 單位電量，Sensor Nodes 每移動一單位所需耗費電量大小為 1 單位電量。而在網路上的重要區域面積為半徑為 50m 大小的圓面積。

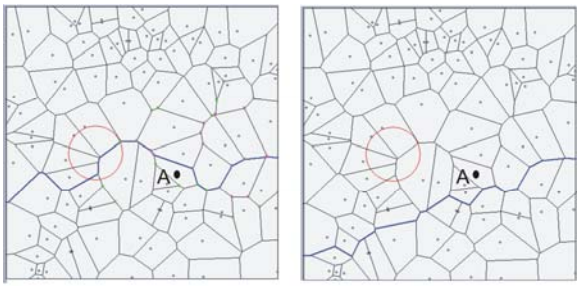
4.2 比較方法

在本實驗中，比較的對象為直覺式的移動方法。所謂直覺式的移動方式，意指移動最靠近重要區域之 Sensor Nodes，並將其往重要區域移動，加強覆蓋重要區域，使入侵者入侵的路徑不會經過重要區域。此一方式，僅考慮重要區域附近的 Sensor Nodes，其移動的位置不需經過詳細的計算，故稱其為直覺式之移動方式。

4.3 實驗結果

圖九(a)為隨機佈點之結果，圖中之圓圈區域為 Vulnerable Area；圖中之線段代表，每個 Sensor Nodes 間所形成之 Voronoi Diagram，其中較粗之線段代表入侵者所行走之路徑。圖九(a)中，入侵者之行進路線，會進入 Vulnerable Area。因此需本篇論文所提出的演算法將會被起動，藉由移動部分 Sensor Nodes 改變目前網路上入侵者路徑。圖九(b)即表示使用本篇論文所提出的 VAPM 演算法，移動後的網路。從圖中可以發現，代表入侵者路徑的粗線段，不再經過網路上的重要區域。而透過兩個圖互相比較，可以發現本論文所提出來之演算法，僅改變位於入侵者路徑上的 Voronoi Vertex *A*，且僅移動極小之距離，便能使入侵者行走的路徑改變，且不經過 Vulnerable Area。

接下來，在實驗中比較網路密度與消耗之電量之關係，在模擬環境 500m*500m 的大小分別佈 50 到 300 個 Sensor Nodes，進行 30 秒的實驗。實驗結果如圖十所示，在 Vulnerable Area 被入侵的時候，若使採用直覺的方式移動感測器時，其消耗的電量明顯消耗的比本篇論文所提出來之方法還要多，且隨著密度增加，整體的耗電量也隨之



(a) 移動前　　(b)移動後

圖九：改變入侵者入侵路徑

提昇;反觀本論文提出之方法，當網路密度增加的時候並不會增加網路整體消耗的電量，此一原因在於，在本篇論文中提出之方法，在移動時考慮選擇耗電量最少的移動組合移動，然而直覺式方法並未考慮到這一點，因此在耗電量上有明顯之差距。

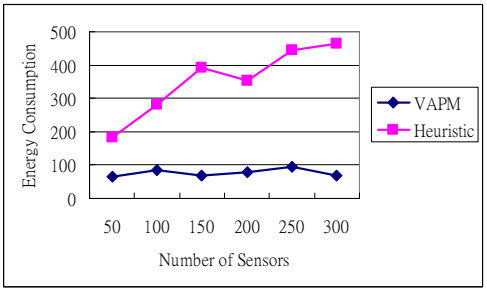
在圖十一的實驗中，在網路上佈建 150 點，分別改變所形成 Vulnerable Area 半徑大小，模擬 Vulnerable Area 大小與電量消耗間關係。實驗結果如圖十一所示，當在相同的 Vulnerable Area 大小下，本篇論文的作法明顯優於直覺式作法，當 Vulnerable Area 變大時，使用直覺式作法的消耗電量隨著 Vulnerable Area 的大小會增加；然而，反觀本論文提出之演算法，隨著 Vulnerable Area 區域的變大，消耗電量並無明顯增加。。

5. 結論

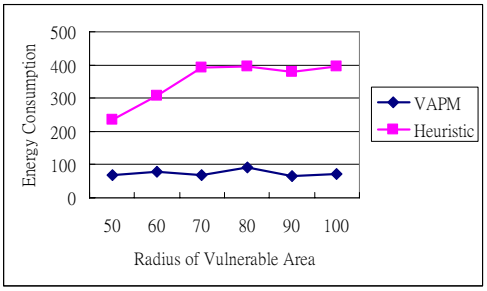
在本論文中，提出一個創新之 Sensor Networks 應用。在環境中假設存在一個 Vulnerable Area，且此一區域不能位於感測能力最薄弱之路徑上。因此在本論文中提出，當此 Vulnerable Area 位於最感測能力最薄弱路徑上時，如何透過移動網路中的 Mobile Sensors 使感測能力最薄弱的路徑改變，且不通過 Vulnerable Area。在本論文所提出之方法，可分為四個部份，首先探討在此環境上哪些 Voronoi Vertices 會對進入 Vulnerable Area 的路徑造成影響。接著探討哪些是可以感測能力最薄弱的路徑改變集合。進一步討論 Sensor Nodes 應如何移動，才能使感測能力最薄弱的路徑改變。最後從集合中挑出一組耗電最少之集合。藉由模擬實驗的結果可以發現，本論文所提出之方法，可以大量減少改變感測能力最薄弱之路徑時所需要之電量，且方法之耗電量不會隨網路密度以及 Vulnerable Area 的密度有所有影響。

6. Acknowledge

本研究感謝中華民國行政院國家科學委員會計畫經費補助(NSC 97-2221-E-032-021)。



圖十. 網路點數與耗電量關係



圖十一. 重要區域大小與耗電量關係

參考文獻

[1]. G. Wang, G. Cao, and T. LaPorta, "Movement-Assisted Sensor Deployment," in *Proceedings of the IEEE INFOCOM, the 23th Annual Joint Conference of the IEEE Computer and Communication Society*, vol. 4, pp. 2469-2479, Mar. 2004.

[2]. R.-H. Gau, and Y.-Y. Peng, T. LaPorta, "A Dual Approach for The Worst-Case-Coverage Deployment Problem in Ad-Hoc Wireless Sensor Networks," in *Proceedings of the International Conference on Mobile Ad-hoc and Sensor Systems* (MASS 2006), pp. 427-436 , Oct. 2006.

[3]. S. Megerian, F. Koushanfar, G. Qu, and M. Potkonjak, "Exposure in Wireless Ad-Hoc Sensor Networks," in *Proceedings of the 7th Annual International Conference on Mobile Computing and Networking* (MobiCom 2001), pp. 139-150.

[4]. S. Megerian, F. Koushanfar, M. Potkonjak, and M. B. Srivastava, "Worst and Best-case Coverage in Sensor Networks," *IEEE Transactions on Mobile Computing*, vol. 4, no. 1, pp. 84-92, Jan. 2005.

[5]. S. Zhou, M.-Y. Wu and W. Shu, "Blocking Vulnerable Paths of Wireless Sensor Networks" in *Proceedings of the IEEE Global Telecommunications Conference* (GLOBECOM 2006), pp. 1-5, Nov. 2006.

[6]. X.-Y. Li, P.-J. Wan, and O. Frieder, "Coverage in wireless ad hoc sensor networks," *IEEE Transactions on Computers*, vol.52, no.6, pp. 753-763, June 2003.

[7]. N. Ahmed, S. S. Kanhere, and S. Jha, "The Hole Problem in Wireless Sensor Networks : A Survey," in Proceedings of the ACM SIGMOBILE Mobile Computing and Communications Review, vol 9, pp. 32-41, 2005.

[8]. X.-Y. Li, P.-J. Wan, and O. Frieder, "Coverage in wireless ad hoc sensor networks," IEEE Transactions on Computers, vol.52, no.6, pp. 753-763, June 2003.