無線感測網路中匯聚節點位置隱私問題

陳豪霆　　胡碩誠　　許智舜
世新大學資訊管理學系　世新大學資訊管理學系　世新大學資訊管理學系
a_pee@hotmail.com　schu@cc.shu.edu.tw　cshsu@cc.shu.edu.tw

摘要

近年來無線感測網路蓬勃發展，而一個感測機器(以下通稱 sensor node)所具備的功能有非常多種，感測節點目前可以感測的項目有 ex:溫度、濕度、角度、加速度和定位的功能[2]。

Sensor networks 開始使用在重要的應用上，因此安全性倍受考驗，sensor networks 所有感測到的資料最後都會流向匯聚節點(以下通稱 sink node)，攻擊者(以下通稱 adversary)透過攻擊 sink node 可以直接得到整個網路的資訊。

我們論文裡提出 Probabilistic Random Path(PRP)，來防止 tracing 的攻擊方式，PRP 機制使較遠的路徑可以得到較高的機率把 message 往 sink node 方向傳送，PRP 採用隨機路由(以下通稱 random routing)，如此一來可以達到保護 sink node 的效果，並且得到較高的網路效能，也加入 fake message 來使反方向的 message 流量較高，讓 adversary 誤以為反方向才是正確的路徑而追錯，讓 PRP 的保護機制更完整。

關鍵詞：source node、sink node、PRP、tracing。

1. 簡介

1.1 研究背景與動機

目前感測網路已經應用在許多生活週遭的環境裡，各方面安全議題的研究仍然持續著[3,5,6,9,11,12]，未來會有更多的應用在任何情境裡，如果朝著很敏感的醫療應用、商業應用或者是軍事[1]議題上發展，資訊安全方面就需要花更多的心思去研究。

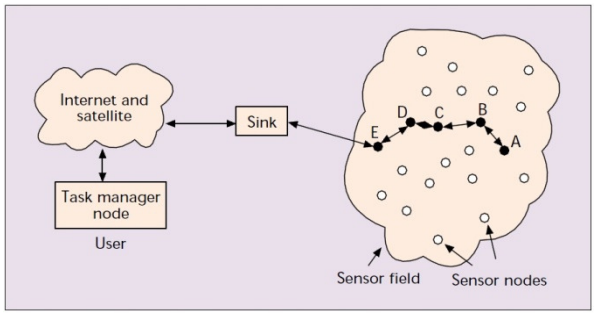

圖 1Wireless Sensor Networks 架構圖[2]

如圖 1 在無線感測網路的環境底下，節點會大量佈置在任何環境裡，適用於每一種情況下的每一種應用，每一個感測節點具有的功能有兩種，一個是事件感測、一個是路由功能。首先，每一個節點可以進行事件感測(sensing)，像是溫度或者是定位的事件觸發，觸發之後先在原始節點(以下通稱 source node)上作一個簡單的資料處理，這個動作是為了減少封包(packet)量的傳送，減少封包量可以達到省電的效果，

而做了簡單的資料處理之後會透過鄰居節點 (neighbor nodes)做一個 hop-by-hop 的傳送，透過每個節點間的資料傳送，把 source node 感測到的資料仍然透過 IEEE 802.15.4 的傳送協定傳送到 sink node，sink node 負責收集所有的 source node 所感測到的資料，在 sink node 彙整之後，sink node 透過 internet 或者是衛星(satellite)傳送到使用者的伺服器端，而使用者的伺服器端可以透過程式來查看這些數據。

而在無線感測網路應用方面，生物學家們為了觀察熊貓最真實的生活又不打擾到熊貓，所以在熊貓身上配戴 sensor node 之後就把熊貓野放回去，藉此學者可以達到使用最少的人力並且達到最完整的觀察效益，但因為獵人們知道熊貓身上有配戴著 sensor node ，所以儘管獵人們無法用肉眼找到熊貓，但是卻可以透過無線網路的攻擊技術去找到 sensor node 的所在位置，也等於找到熊貓的所在位置，獵人透過追回攻擊(以下通稱 tracing)的技術去找到 sensor node，每個 adversary (指獵人) 身上配戴天線(antenna)，antenna 可以接收無線網路中的封包資訊。因為無線網路天生暴露在開放式的環境底下，所以獵人可以使用天線去擷取封包，封包裡頭包含傳送端節點號碼 (sender node ID)和接收端節點號碼(receiver node ID)，藉此 adversary 可以知道上一個傳送資料過來的節點在哪裡，並且移動到上一個傳送資料過來的節點，透過不斷的重複這個動作，adversary 只需要花點時間成本就可以不用肉眼也能輕易的找到熊貓的所在位置。

如果是使用在軍事上[1]，那安全問題就更嚴謹了，今天在戰場上佈置了感測敵人是否靠近的節點、我方士兵的定位節點和戰場災情控制節點等等...而這些資料經過節點本身簡單的資料處理後，終究會傳送到 sink node，而 adversary 最簡單最輕鬆的攻擊方式就是直接攻擊 sink node 做資料的擷取，就不必去對整個網路做攻擊，而只需要攻擊一個節點對於 adversary 來說，是最省成本的攻擊方式。

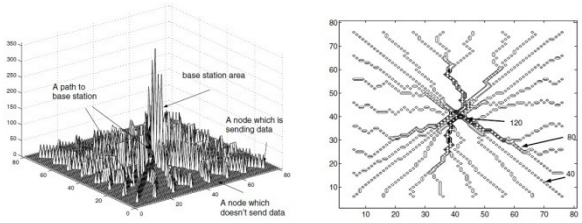

圖 2 Sink 周圍的封包傳送率較高[4]

如圖 2 所示， sink node 附近的資料流量會最大，adversary 利用所配戴的天線去做封包的收集，並且加以分析，就可以得到 sink node 的所在位置。如果 sink node 被發現並攻破，那整個戰場上的資訊將會被敵人全數取得，會使得我方陣營陷入不利的情況。

1.2 研究目的

以上兩個例子分別是在講 source node 和 sink node 的位置被發現後的安全性問題，由此可知，在無線感測網路底下，節點位

置隱私問題 (Location Privacy Issues)是很重要的。

而本論文的目的就在於保護 sink node 的位置，透過一些安全機制來使得 adversary 需要花更多的時間和成本來做攻擊，導致 adversary 的攻擊不符合成本效益而減少攻擊動機，並且在達到保護效果時同時改善網路傳輸效能。

1.3 論文架構

此篇文獻將分為以下四個章節來說明：第一章為緒論，探討本論文的研究動機、研究目的、研究範圍以及論文架構，說明在無線感測網路下節點位置隱私的重要性。第二章為文獻探討，將相關領域學者所提出的安全認證機制及網路環境作分析探討，對應本研究欲解決的問題。第三章為相關背景與技術,著重在於sensor背景的介紹、應用、節點位置隱私攻擊方法和節點位置隱私保護方法。第四章為本文的研究機制，深入的介紹本文所提出來的機制，使用本機制去達到更高效益的安全性能與執行效能，並且分析效能分析。

2. 文獻探討

本章節將探討各學者的研究機制[7,8,13]，整理各機制的優缺點，學習各機制的優點，並改善各機制的缺失，來提升本研究的機制，使本機制能較各學者的機制更為完整。

2.1 以 ring-based 去保護 source 節點的位置隱私

在此篇文獻裡[8]，學者 Yun Li 和 Jian Ren 提出了三個階段的保護方式去保護 source-location。

第一階段：事件觸發後，由 source 所產生的 data 會隨機在整個 sensor network 裡面選擇多個 sensor node 當作 intermediate node，然後傳送這個資料到這個 randomly selected intermediate node (RRIN)，這個階段提供了 source-location privacy 的保護。

第二階段：在這個階段裡，這個 data packet 會透過傳送到 network mixing ring(NMR)和其他的資料混合在一起，這邊提供了網路層 source-location privacy 的保護。

第三階段：最後在這個環狀裡面流動的資料後透過某一些特定的節點把資料傳送到 sink node。

整個 sensor network 被分割成整齊的小區塊 (small grids)，而 sensor node 被隨機散佈在這些 grid 裡面，每個 grid 裡面都會有一個 header node，而且整個 sensor network 的每個 sensor node 是可以互相連接的。

每一個節點都知道自己和鄰居節點的位置，整個網路的位置的資訊可以透過廣播(broadcast)去更新。

此篇文獻的攻擊者試圖使用 traffic analysis 和 tracing 去找出 source node 的位置，攻擊者具有以下幾點特徵:(1)Adversary 具有強大的硬體設備足以去分析和記錄資料，可以很輕易的發現 intermediate node 的位置並且移動到旁邊(2)Adversary 不會去對節點做竄改或者是破壞的動作，因為這樣很容易被發現攻擊的行為，這邊的攻擊者只是竊取資料。(3)Adversary 可以分析和傳輸訊息，換言之，adversary 可以了解整個網路的傳輸運作。

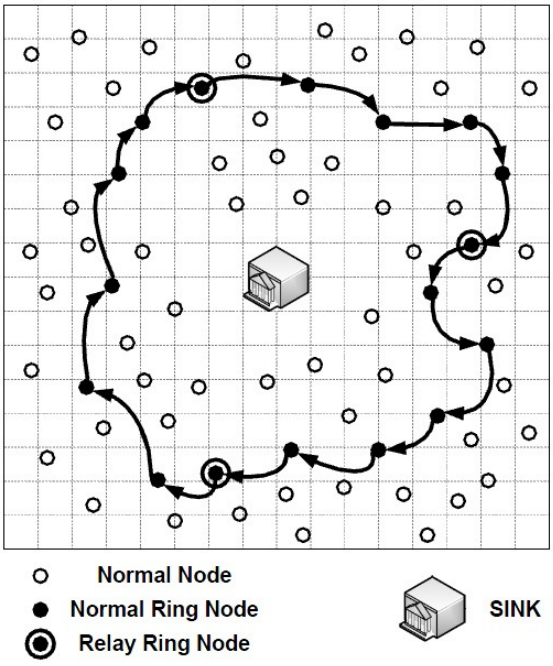

圖 3 Ring-base[8]

如圖 3 所示，ring 是由多個 header nodes 組成，normal node 負責產生 data，而 relay ring node 不同 normal 在於 relay ring node 會產生一個 vehicle message，這個 vehicle message 會在這個由 normal ring node 和 relay ring node 組成的 ring 裡順時針 routing。

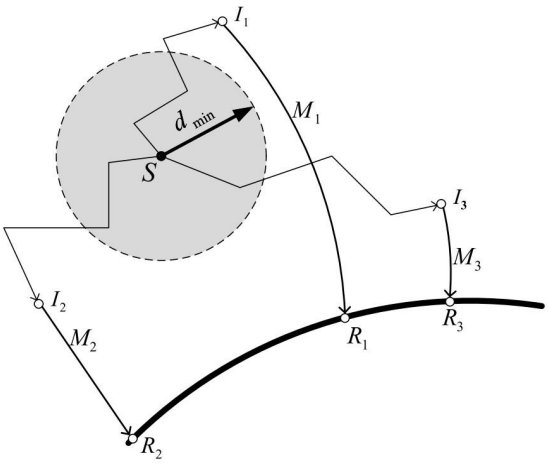

圖 4 Source node 挑選 intermediate node 時加入 dmin 值[8]

如圖 4 所示，I1、I2、I3 分別表示 intermediate1、2、3，normal node 挑選 intermediate node 的時候，如果挑選太接近 normal node 的 intermediate node，由於 intermediate node 離 normal node 太近，所以當 intermediate node 被發現時則很容易就可以透過 tracing 去找到這個 source node 的位置，所以這篇文獻設了一個 d_{min} 的最小範圍，在 normal node 周圍 d_{min} 的值裡面不會去挑選 node 當作 intermediate node，此方法可以達到預防 tracing 的效果，當 data 傳到 intermediate node 的時候，再使用最短路徑方式傳送 data 到 ring 裡面，並且儲存在 normal ring node 或者 relay ring node 裡

傳送到 ring 裡面之後，會由圖 3 中的 relay ring node 產生 vehicle message，vehicle message 會在這個 ring 裡面做 hop-by-hop 的傳輸，並且沿路接收儲存在 normal node

裡的 data，當接受到 data 後依然繼續 hop-by-hop 的向下一個 node 移動，直到移動到 relay ring node，則 relay ring node 有一定機率 p 採用最短路徑把 data 傳送到 sink node 端。

雖然可以透過 routing through a random intermediate node 和 ring 的機制來保護 adversary 使用 tracing 方式去追到 source node，但是在執行效能方面，由於 ring 裡面的 node 傳送使用率比較高，所以 ring 的 node 壽命上一定會大大縮短，會提早造成網路的損壞，另外， data 都往 sink node 方向送並且 ring 區塊的傳送率特高，所以 adversary 使用 traffic analysis 去長時間分析，很容易就可以找到 sink node 在哪個區塊，並沒有達到保護 sink node 的效用。

2.2 以 locational angle 去保護 source 節點的位置隱私

此篇文獻中[13]提到把無線感測網路使用在觀察動物或者是戰上，動物或者士兵會配戴著一個 source node，因此 source node 的位置隱私便顯得非常的重要，一旦 source node 被 adversary 發現，則動物或者士兵便處於一個非常危險的處境內。

此篇文獻中採用 tracing 的攻擊方式，假設 adversary 知道 sink node 的點在哪裡，從 sink node 開始追蹤，當 adversary 竊聽到傳送過來的 message 時，便會去找出是哪個節點傳過來的，並且移動到這個傳送 message 的節點旁邊，等待下一個傳送過來的訊息，重複做這些事情就可以找到 source node，整個 tracing 攻擊的演算法如圖 5。

```
Attacker =sinkAddr;     //Attacker starts from sink
While (Does not capture the source ) do
      Listen (next_msg);       //Continue listening new message
      if (ReceiveMessage())
            if (IsNewMessage(msg)) then       //Detect a new
message
                  next location = GetImmediateSender(msg);
                  MoveTo(next location);
//Move to the message sender and repeat tracing strategy
```

圖 5 Tracing 攻擊方式的演算法[13]

此篇文獻中提出 phantom routing with locational angle (PRLA)為主要機制，PRLA 分為兩個階段，第一個階段會由 source node 找出一個 phantom node 並且採用 random walk 的方式隨送 message 到 phantom node，第二個階段被選擇的 phantom node 會採用最短傳輸路徑把 data 傳送到 sink node，在第一階段使用 random walk 時可以延長 source node 被 adversary 發現的時間，也增加被發現的困難度。

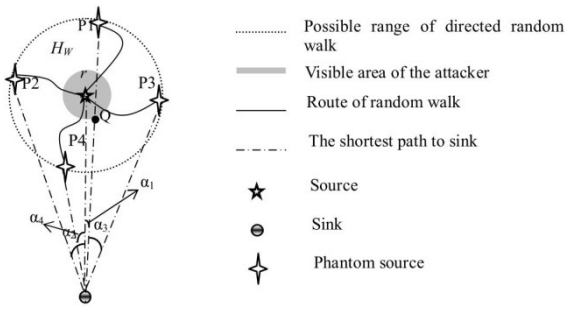

圖 6 Phantom routing with locational angle (PRLA)[13]

圖 6 中以 r 為半徑的陰影區塊表示 adversary 如果在這個區塊內，便可以很清楚的知道 source node 位置所在，而 source node 在半徑 r 之外選擇了數個 phantom source 當作 intermediate node，這些 phantom

source 接收到資料之後採用最短路徑傳送資料到 sink node，而如果 source node 選擇 P1 這條路線傳送資料，當 adversary 從 SINK 端開始 tracing 回 source 端時，會經過以 r 為半徑的危險區域，adversary 在 Q 點的時候就可以找到 source node，所以 P1 這條路徑雖然增加了安全成本卻沒有增加安全性，是為一條浪費的路徑，phantom source P2、P3 和 P4 則不會，為安全路徑，如圖 7 所示，phantom source A 到 phantom source B 之間是為浪費路徑，增加了成本卻沒有增加安全性是我們非常不樂見的一件事情，所以如何去減少浪費的路徑就是本文獻的主題。

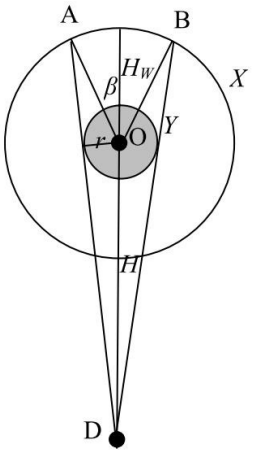

圖 7 PRLA 的浪費路徑圖[13]

此篇文獻主要比較對象是 phantom single path，在執行效能的比較上兩者沒有差異，但是安全效能上比 phantom single path 高出許多，尤其是在 source node 傳送資料到 sink node 的總 hop 數增加的時候，PRLA 的安全性越高。

2.3 在大型的 WSN 網路底下保護節點位置隱私

此篇文獻[7]不同於可以同時保護 sink node 和 source node，在文獻裡面提了 Location Privacy Support Scheme(LPSS)，這個方法可以配合 delivery delay 產生多種路徑，文獻又提到如果跟其他防禦機制比較的話，在同樣的 delivery delay 或者是 energy cost 下，LPSS 都擁有更強的安全性，而且如果把 source node 和 sink node 的距離拉長，安全性會更高。

文獻中的系統假設只有一個 source node 和一個 sink node，source node 會定期發送 message 到 sink node，在整個無線感測網路的初始配置階段，sink node 會廣播出去一個 beacon，這個 beacon 包含 sink node 的 ID 和每個節點到 sink node 的 hop 數，當整個 beacon flooding 結束後，每個節點知道鄰居節點跟自己的角度是幾度，這個角度是用來判斷並且歸類自己的鄰居節點離 sink node 比自己近還是比自己遠，每次傳 message 到 sink node 的時候就會以機率去選擇下一個節點要選擇離 sink node 近的還是離 sink node 遠的，選擇離 sink node 近的機率會比較高。

文獻裡面提到 adversary 並不會去對節點做竄改或者打擾性的攻擊，只會擷取資料，並且 adversary 是更聰明的，他們具有頻譜分析儀(spectrum analysis)[7]可以分辨 message 從哪個方向傳送過來。

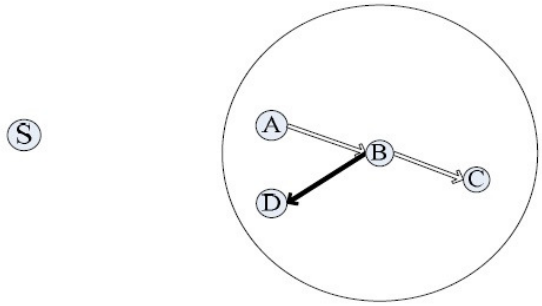

圖 8 裝有 spectrum analysis 的 tracing attacker[7]

如圖 8 所示，當 source node 產生資料並且傳送到節點 A 之後，此時，adversary 在節點 B 旁邊等待並且偵測 message 來哪裡送過來，adversary 只能偵測 message 從哪裡傳送過來，並不能偵測送往哪裡，所以當 adversary 知道 message 是從節點 A 時，他並不知道下一個節點的正確路徑是節點 C，但因為 sensor node 是以廣播方式做傳輸，所以當節點 C 接收到節點 B 的 message 後，為了往下一個節點傳送，所以也會採取廣播往下一個節點傳送，所以節點 B 也會接收到來自節點 C 的廣播，adversary 由此判斷下一個路徑是節點 C。

為了防止 Rate-monitoring 攻擊，所以此篇文獻加入 fake packet injection 的防禦機制，如圖 8 節點 B 傳送 message 到節點 C 同時產生一個 fake packet 傳送到節點 D，所以 sink node 附近的資料傳送率不會特別高，所以 adversary 無法很快的去發現 sink node 所在位置。

但一開始佈置 sensor node 時，每個節點都知道自己跟鄰居節點與 sink node 之間節點的角度，以此用來歸類每個鄰居節點是屬於離 sink node 較遠或較近，用機率 p 去挑下一個節點應該傳送往哪個類別的節點，而為了不使 source node 傳送資料到 sink node 的時間太久，所以被歸類在離 sink node 較近的節點被挑選中的 p 較高，因此 routing path 可以不斷的改變，使 adversary 追蹤不到正確的方向應該是哪裡。

3. 網路模型與攻擊模型

3.1 網路模型

在 sensor networks 網路環境底下，sink node 是所有 source node 偵測到事件後產生 message 的最終傳送目的。

Sensor node 被較平均的佈署在整個網路裡頭，在自己的通訊半徑範圍內的節點稱為鄰居節點。

在做人工佈署階段時，每個 sensor node 會擁有自己的 node ID 和座標值，node ID 和座標值由佈置者去做 ID 編號設定，設定 node ID 與座標值是為了辨識是由哪個 sensor node 產生事件觸發。

所有的 sensor node 把鄰居節點分成兩類，near node 與 far node，在 sensor networks 佈署階段時候，sink node 會廣播 beacon 給鄰居節點，每個 sensor node 收到 beacon 後繼續做廣播的動作往鄰居節點傳送，每傳送一次 beacon 裡的 hop count 數加 1，而從同一個鄰居節點收到兩個不同的 hop count 數時只保留 hop count 較小的值，此為最短

路徑，透過 hop count 數可以使 sensor node 知道自己與鄰居節點到 sink node 的距離，sensor node 與自己的鄰居節點做比較，如果鄰居節點的 hop count 數比自己小，則被歸類為 near node，表示離 sink node 比較近，如果 hop count 數比自己大或者剛好等於自己，則被歸類在 far node。

3.2 攻擊模型

整個網路裡頭只有一個 adversary，而 adversary 為了要準確的分析資料去做 tracing 和 traffic analysis[10]攻擊，因此需要有很大的資料儲存空間，並且具有強大的運算能力去做分析，當 adversary 發現自己在做 tracing 攻擊時候走錯路徑，有辦法回到前一個走過的 sensor node。

Adversary 配戴有天線，可以竊聽和攔截 message，並且知道 message 是從哪一個 sensor node 傳送過來，如此一來 adversary 即可以做 tracing 的攻擊。

因為對 sensor node 做節點竄改攻擊很容易被防禦者發現並且快速的做應對，因此 adversary 不會去做此類的主動攻擊，adversary 待在兩個 sensor node 之間並且利用天線去攔截 message，不去對 message 做破解，因為攻擊者主要目的是找到 sink node 的節點位置而不是去取得 source node 所感測到的資料，因此 adversary 不需要有破解金鑰的能力。

4. 節點位置隱私的保護機制

本章將介紹本研究的機制。4.1 節為本研究機制之簡介，說明相關背景與目的，4.2 節為本研究機制之實行方法與機制完整流程，4.3 節為本研究所預期達到之結果，描述了安全效能分析與執行效能分析。

4.1 系統簡介

本研究的系統環境建制於無線感測網路機制底下，在無線網路環境底下是相當容易受到攻擊的，攻擊又有分為主動式(竄改節點、放置惡意節點…)和被動式(竊聽)，本研究探討被動式攻擊之防禦機制，目的在於保護 sink node 的位置隱私，因為在 sensor networks 底下，通常 sink node 是所有感測到的資料所匯集之處，所以位置隱私極為重要，又因為 sensor networks 電力提供相當不足，所以不考慮會大量消耗電力的複雜加解密運算，而把重點著重於使用路由方式來達到保護目的。

本研究機制提供 tracing 的防禦機制，本論文著重於保護 sink node 端，除了使用了文獻中的 random routing 和 fake message，還另外加入了機率的機制，每個節點將自己的鄰居節點分成兩類，further node 和 closer node。跟 source node 比較起來，比 node N 遠的 node 被稱為 further node，反之，跟 source node 比較起來，比 node N 近的 node 被稱為 closer node。從 source node 開

始到 sink node 之間的距離越遠，把 message 傳送往 closer node 的機率越高，往 closer node 傳送 message 的機率越高則 message 越快抵達 sink node，並讓 further node 加入發送 fake message 的機制，誘導 adversary 走向錯誤的路徑，遠離 sink node。

4.2 本文機制

Sensor networks 佈置分為兩個階段，第一個階段選擇一個區域隨機平均佈置一些固定的 sensor node 和一個固定的 sink node，sink node 佈置在整個 sensor networks 的中央。第二階段一開始 sink node 會對周圍鄰居節點發送 beacon，beacon 用來記錄每個 sensor node 到 sink node 所需要的 hop count 數，從 sink node 發送 beacon 裡的 H_{count} 初始值為 0，每往一個 sensor node 傳送，H_{count} 值加 1，又因為 beacon 是採用廣播方式發送，所以一個 sensor node 可能會接收到同一個鄰居節點發送過來兩次 beacon，這時候 sensor node 將較大的 H_{count} 值刪除，保留最小的，因此每個 sensor node 知道自己與 sink node 之間所需要最短的 hop count 數，sensor node 與鄰居節點交換訊息就可以知道鄰居節點到 sink node 所需要的 hop count 數，藉由 hop count 數，可以把 sensor node 的鄰居節點分成 far group 與 near group，hop count 數與自己相同的鄰居節點則被歸類在 far group 裡。

在 sensor node 傳送 message 到下一個 sensor node 時，adversary 在 sensor node 旁邊採用 tracing 的攻擊方式，adversary 會經過一段時間後去分析哪一個 sensor node 的 message 流量較多，由此確認正確的下一個 sensor node，並將 adversary 本身的位置移動到 adversary 認為是正確路徑上的下一個 sensor node 上並且繼續等待 message 的分析，經過重複的動作，adversary 最終可以找到 sink node。

為了防止 adversary 得到正確的追蹤路徑，我們不只把 message 往 sink node 方向做傳送，也把 message 往 sink node 的反方向做傳送，使 adversary 需要花更多的時間去做分析，或者在短時間內無法找到 sink node 的位置，而達到保護 sink node 位置的效果。

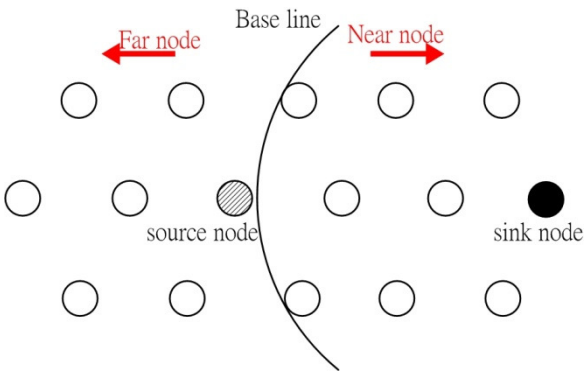

圖 9 far node 和 near node 分類

Source node 感測到資料之後把處理過後的 message 採用 Probabilistic Random Path (PRP)轉傳到下一個節點。如圖 9，這個節點的選擇是以節點本身與本身之鄰居節點的 H_{count} 值做比較，把鄰居節點分成兩類的 far group 和 near group 中去挑選 node

做機率的傳送，選擇把 message 往哪個類別的節點傳送，且每個 message 的最終路徑目的為 sink node，R_p 為 sensor node 選擇將 message 往 near node 傳送的機率值，而往 far node 傳送的機率值則為 1-R_p。

通常選擇 near node 為下一個傳送節點的機率會比 far node 高，也就是 R_p 值必須大於 50%，如此一來 sensor node 才有辦法將 message 順利的往 sink node 方向傳送，又因為每個 sensor node 與 sink node 的距離都不一樣，對於 source node 離 sink node 較遠的情況下，message 傳送會需要較長時間，將無法達到較佳網路效能，為了達到較佳網路效能，我們的機制會依照目前 sensor node 到 sink node 所需的 hop count 數去調整機率 R_p，H_{count} 值越高的 sensor node，則會擁有較高的 R_p 值，反之，當 sensor node 越接近 sink node 時會擁有較低的 R_p 值。

在我們的機制裡，為了防止 tracing 攻擊，sensor node 將 message 往 near node 傳送的機率 R_p 平均分配給 near group 的所有節點 N_n，則 near group 裡每個 near node 被挑選為下一個傳送 message 的節點機率為 $\frac{R_p}{N_n}$。sensor node 將 message 往 far node 傳送的機率 1-R_p 平均分給 far group 的所有節點 F_n，但為了讓 adversary 追到錯誤的 sensor node，因此我們故意讓 far group 裡面某些 far node 被挑選為下一個傳送節點的機率大過於 $\frac{R_p}{N_n}$ 的機率，如此一來 adversary 經過某段時間分析後，會發現我們故意虛設的某些 far node 的 message 傳送率比較高，就會被誘導走向錯的方向，所以我們加入數值 F_d，F_d 是指在 far group 裡不被挑選為下一個傳送 message 的 far node，則 far group node 裡每個 far node 被挑選為下一個傳送 message 的節點的機率為 $\frac{1-R_p}{F_n-F_d}$，經過調整 Fd 值我們可以控制 far group 裡用來傳送 message 的 sensor node 數量。

在 source node 離 sink node 較遠的時候，R_p 值會很高，使 message 較為順利的往 sink node 傳送，也因為 R_p 值會比較高，因此 1-R_p 值會較低，這樣的數值會影響到 $\frac{R_p}{N_n}$ 與 $\frac{1-R_p}{F_n-F_d}$ 的表現，但我們理想的狀況是 $\frac{1-R_p}{F_n-F_d}$ 加入 fake message 之後的值會大於 $\frac{R_p}{N_n}$ 值，為了達到此理想狀況，我們需要加入 fake message 來使 $\frac{1-R_p}{F_n-F_d}$ 值會大於 $\frac{R_p}{N_n}$ 值，當一個 real message 從 near group 裡的 near node 往 sink node 方向傳送時，far group 有機率 FM_c 產生 fake message，但為了讓某些 far node 的 message 傳輸率較高去誘導 adversary 走向錯的路徑，所以當 near node 傳送一個 message 時候，far node (F_n-F_d) 產生 fake message，因此從 far group 裡被挑選中的 far node 產生 fake message 的機率為 $\frac{R_p}{F_n-F_d}FM_c$，加入 fake message 目的是為了 $\left(\frac{1-R_p}{F_n-F_d}+\right.$

$\frac{R_p}{F_n-F_d}FM_c\Big) > \frac{R_p}{N_n}$ ，因此 F_d、FM_c、R_p 值的設定會影響整個 sensor network 的效能和安全性。

4.3 效能分析

此章節用來描述在我們的機制裡頭所預期該有的成果，並且與文獻裡的 all random routing path 與 LPSS[7]做比較，而比較的項目有 packet delay、Delivery rate、attacker's steps moved 和 energy cost ration。

4.3.1 安全性分析

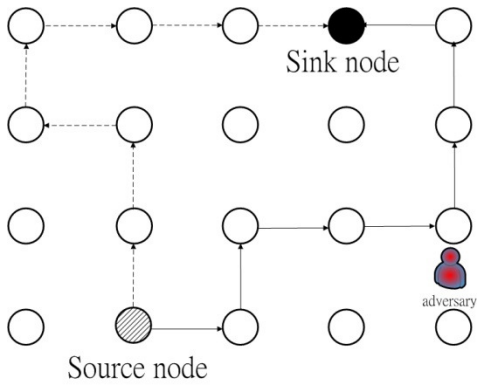

圖 10 random path

因為傳送路徑都採用 PRP，而 PRP 採用 random path，如圖 10 所示，攻擊者就算追到上一個傳送 message 過來的節點，但因為 source node 採用 random path，所以下一次 message 的路徑不會是同一條路徑，因此 adversary 無法繼續往前追到 sink node。而我們所設定的 adversary 擁有做短時間內流量分析的能力，分析 message 往哪個方向移動，就可以輕易的使用 tracing attack 去追到 sink node 的位置。

加入 fake message 使 far group 裡 1-F_d 個 far node 的$\frac{1-R_p}{F_n-F_d}$機率值大於每個 near node 的$\frac{R_p}{N_n}$機率值，如此一來，adversary 在做流量分析時候，會發現某幾條由 far node 所組成的路徑的 message 傳輸量特別高，會誤以為由 far node 所組成的路徑是正確的，而被誘騙往反方向做移動，adversary 會離 sink node 越來越遠，藉此達到保護 sink node 的目的。

4.3.2 封包延遲比較

在 packet delay 方面，all random routing path 採用完全隨機的路徑傳送 message，把時間拉長來觀察的話，往 sink node 傳送 message 的機率只有一半，而文獻[7]中的 LPSS 機制雖然設定大於 50%的機率把 message 往 sink node 傳送，但每個中間負責轉傳 message 的 sensor node 把 message 往 sink node 傳送的機率都一樣，因此在較大的 sensor networks 環境底下，如果一開始 source node 設定的機率太低，會造成 packet delay 很大，而我們的機制 Probabilistic Random Path(PRP)在每個節點都會重新計算一次跟 sink node 的距離，由距離去調整挑選 near node 做傳送 message 的機率，距離越遠 message 往前傳送的機率越高，如此一來不用擔心離 sink node 很遠的 source node 往前傳送的機率很低，而使網路路徑很長。

4.3.3 封包抵達率比較

如同 packet delay 裡提到的，在我們的 PRP 機制裡，把 message 往 sink node 傳送的機率會比 all random routing path 高，因此在 delivery rate 的表現會比 all random routing path 好，而跟 LPSS[7]比較的話，source node 離 sink node 越遠的情況下，PRP 的表現會越好。

4.3.4 攻擊者花費路徑成本

adversary 需要花更多的 steps moved，則機制的保護越高。由於 all random routing path 往前傳送 message 的機率只有一半，而且採完全隨機路由，因此 adversary 有一半的機率會往 far node 去追蹤，因此在 attacker's steps moved 的表現，random path 會比 LPSS 和 PRP 好，但如果在較大的 sensor networks 環境底下，則 PRP 不會比 all random 差太多，且比 LPSS 擁有更好的保護強度。

4.3.5 能量消耗

PRP 與 LPSS 都加入 fake message 的發送，因此在 energy cost 會比 all random 差，而在 LPSS 機制下，message 往前傳送的機率越高，則往反方向產生 fake message 的機率越高，也代表 energy cost 越高，而我們的機制 PRP 則不需要產生太多的 fake message，因為我們產生的 fake message 量只需要達到能使某幾個 far node 的 message 傳送機率比 near node 高即可，因此比 LPSS 所需要產生的 fake message 量還少，因此在 energy cost 的表現，PRP 優於 LPSS。

5. 結論與展望

本篇論文裡我們提出 Probabilistic Random Path (PRP)機制，使 message 不會只往 sink node 方向傳送，也會將 message 往反方向傳送，來防止 adversary 使用 tracing 攻擊方式來攻擊 sink node，並且當 sensor node 離 sink node 越遠，message 被往前傳送的機率越高，藉此得到更好的網路傳輸效能。也加入 fake packet 增加反方向的某幾條路徑 message 量，使 adversary 追錯路徑，來達到更有效果的 sink node 防護方式。

在未來的工作，我們將利用 NS2 網路模擬軟體，來驗證所提出機制的效能，並且與文獻中其他機制做效能分析與保護強度比較，以實際數據資料，進一步證實本機制的優點。

參考文獻

[1] Lisa Ann Osadicw and Rajani Muraleedharan, *An Intrusion Detection Framework for Sensor Network Using Honeypot and Swarm Intelligence*, MobiQuitous '09. 6th Annual International, 2009, pp. 1-2.

[2] Ian F. Akyildiz, Weilian Su, Yogesh

Sankarasubramaniam and and Erdal Cayirci, *A survey on sensor networks*, Communications Magazine, IEEE, 2002, pp. 102-114.

[3] Yanping Cong, Guang Yang, Zhiqiang Wei and Wei Zhou, *Security in Underwater Sensor Network*, International Conference on Communications and Mobile Computing, 2010, pp. 162-168.

[4] Jing Deng, Richard Han and Shivakant Mishra, *Countermeasures Against Traffic Analysis Attacks in Wireless Sensor Networks*, Security and Privacy for Emerging Areas in Communications Networks, 2005, pp. 113-126.

[5] Marco Gruteser, Graham Schelle, Ashish Jain, Rick Han, and Dirk Grunwald, *Privacy-Aware Location Sensor Networks*, Proceedings of the 9th conference on Hot Topics in Operating Systems, 2003, pp. 1-5.

[6] Ying Jian, Shigang Chen, Zhan Zhang and Liang Zhang, *A Novel Scheme for Protecting Receiver's Location Privacy in Wireless Sensor Network*, IEEE Transactions on Wireless Communications, 2008, pp. 3769-3779.

[7] Lei Kang, *Protecting Location Privacy in Large-Scale Wireless Sensor Networks*, ICC 2009, 2009, pp. 1-6.

[8] Yun Li and Jian Ren, *Mixing Ring-Based Source-Location Privacy in Wireless Sensor Networks*, Computer Communications and Networks, 2009, pp. 1-6.

[9] Yun Li and Jian Ren, *Source-Location Privacy through Dynamic Routing in Wireless Sensor Networks*, INFOCOM, 2010, pp. 1-9.

[10] Xi Luo, Xu Ji and Myong-Soon Park, *Location Privacy against Traffic Analysis Attacks in Wireless Sensor Networks*, Information Science and Applications (ICISA), 2010, pp. 1-6.

[11] Edith C.-H. Ngai and Ioana Rodhe, *On providing location privacy for mobile sinks in wireless sensor networks*, MSWiM'09, pp. 1-8.

[12] Stefan Ransom, Dennis Pfisterer and Stefan Fischer, *Comprehensible Security Synthesis for Wireless Sensor Network*, Proceedings of the 3rd international workshop on Middleware for sensor networks,2008,pp. 19-24.

[13] Wei-ping WANG, CHEN Liang and WANG Jian-xin, *A source-location privacy protocol in WSN based on locational angle*, Communications, 2008. ICC '08. IEEE International Conference, 2008, pp. 1630-1634.