無線隨意網路之蟲洞攻擊研究與防禦

Research and Prevention of Wormhole Attacks in Wireless Ad-Hoc Networks

任上鳴　賴溪松
國立成功大學電腦與通信工程研究所
E-mail：elecal@crypto.ee.ncku.edu.tw　laihcs@eembox.ncku.edu.tw

摘要

無線隨意網路是一種新興的網路系統，依靠著自我組織的能力在沒有基礎設施的環境當中，可以快速而有效率地形成一個通訊網路。但在這種型態的網路當中，因為通訊完全依靠無線傳輸，就容易存在許多安全性的問題。其中，蟲洞攻擊是一種藉由快速的傳輸方式以取得相較於正常路由更好的傳輸參數，進而掌控路由權利所產生的攻擊。近年來有諸多針對此問題提出解決方案，如：Hu 等人提出的封包控制方法、Wang 等人提出的視覺化方法以及 Lazos 等人提出了圖論方法…等，來偵測蟲洞的存在並避免之。他們皆是由管理者的角度下手，仰賴一些特殊的硬體或是大量的運算，並著重於偵測蟲洞的所在位置。本論文提出一個有效率的機制，是由使用者的角度來避免明顯可能存在危害的路由，即可達到較上述機制更為良好的安全效果。

關鍵字：蟲洞攻擊、無線隨意網路、路由安全。

Abstract

The wireless Ad-hoc network is a kind of newly risen network system. Nodes in the network can form a communication system without infrastructure with the ability of self-organization. There are serious security issues in this kind of network due to its wireless transmissions. For instance, the routes which go through a wormhole tunnel formed by attackers may have better transmission parameters than normal ones, so that malicious nodes can easily have the right of routing. Until now, many researches against this problem have been proposed. For examples, Hu et al. presented a method of packet leashes; Wang et al. constructed a visualization system, etc. Some special hardware or enormous computations are needed in most of these methods. In this paper, we will propose an efficient mechanism from users' viewpoint to avoid some unsafe routes, and have better efficiency than the mechanisms we referred in this paper.

Keywords：Wormhole attack, Wireless ad-hoc networks, route security

1.簡介

近年來，隨著資訊科技的進步，以及可攜式設備的技術日益成熟，便於攜帶的各式手持裝置，例如行動電話、個人數位助理(personal digital assistant, PDA)、筆記型電腦、車用電子設備等等，都漸漸開始出現對於網路的需求。所以，這些設備要如何與網路相連，就成為一個重要的課題。

在傳統的通信網路架構中，都是屬於具有基礎架構的。例如：行動電話應與基地台連接，PDA、筆記型電腦則可與無線網路基地台的存取點(access point, AP)或藉由 RJ-45 網路線與外界連接。當可移動設備離開了存取點的天線範圍之後，就失去了通訊的能力。

無線隨意網路(wireless ad-hoc network, MANET)[2]就是一種可以獨立經由一個自我組織(self-organization)過程所形成的網路。其通訊的環境不需基礎架構，節點(node)間藉由互相協助傳遞封包的方式來建構一個行動網路。

無線隨意網路中的所有節點皆可視為路由器，在傳遞資料時，節點間需要互相協助傳遞資料，所以除了來源端與目的端之外，封包還會被其

他的節點所接收到。不僅如此，由於無線隨意網路利用電波傳遞所有訊號，故在通訊範圍內，不論是否為路由經過的節點，皆可收到封包內容，大幅增加了洩密的可能性。而這些節點中可能存有惡意節點，就會產生安全性的問題。

目前已知最基本的無線隨意網路攻擊種類主要有三種：資料竄改、竊聽與阻斷服務攻擊。這三種類型的攻擊在有線網路中較不易實現，因為它可能需要藉由入侵主機的舉動方能達成，但在無線隨意網路中，惡意節點可以扮演著球員兼裁判的角色，其電腦可能就是資料流經的路由器之一，故要採取攻擊相當容易。

在愛因斯坦的廣義相對論中，提到了兩種天體，其中一個是黑洞，不斷的吸收包含了光線的物質；另一個則是白洞，相對於黑洞，將物質迸射而出。除此之外，有一詞「蟲洞」，指的是將一物體如黑洞般吸入，再將該物轉移至其它地方，像白洞般發散出來。在無線隨意網路中，存在有黑洞及白洞攻擊，也有結合了兩者的蟲洞攻擊，它能使封包從一個節點進入，經由一特殊管道到達另一地，這個管道可以是有線網路或大功率指向天線…等據有較佳傳輸距離及效能的通路，我們稱之為「隧道」(tunnel)，而隧道的兩端即為串通的惡意節點對。

這樣的傳輸手法可以避免一些不要必要的傳輸時間，例如：在 AODV[10]協定中，廣播 RREQ 封包需要經過節點間的傳遞，最後才能到達目的端，然而這些節點若是較為密集，就可能造成許多不必要的碰撞，影響傳輸的時間。在 802.11 規格書中，對這種狀況採用了 CSMA/CA 的機制，在偵測到碰撞時必須以 backoff 的方式等待傳輸，故在碰撞區域重疊嚴重時，會產生極大的延遲。此時蟲洞傳輸手法就如同為封包搭建了一條通往遠方的專線，使封包迅速抵達另一地。

然而，此種傳輸手法看似有效率，但若通道的兩端為惡意節點，此種傳輸手法就成為了有效的攻擊手法。以 AODV 標準來說，當來源端接收到了回傳的 RREP 封包之後，為了達到較佳的效率，將選擇較短的傳輸路徑，也就是 RREP 封包內跳躍數(hop count)欄位值較小者。若是單一的惡意節點，必須竄改此欄位的值以取得路由權利，然而在蟲洞攻擊手法中，不須在封包上做任何手腳，即可因為較佳的傳輸參數，輕易取得路由權，可參考圖 1。此種攻擊手法難以藉由保護封包資訊來預防。因為蟲洞攻擊藉由使用特殊的傳輸方式，確實地減少了所經過的節點數。

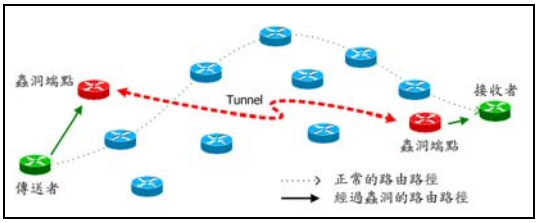

圖 1 蟲洞攻擊示意圖

蟲洞攻擊可以藉此取得大部份路由權利。若封包內容未經加密，則惡意節點可監聽、竄改封包；即使內容經過加密，攻擊者仍可以進行阻斷服務攻擊(Denial of Services, DoS)，當來源端認為路由失效，重新尋找路由路徑時，攻擊者可以再次取得路由權利，並再次阻斷服務，對於無線隨意網路的資料傳遞具有極大的影響力。

除了上述的三種攻擊外，蟲洞也可能引發其它的困擾，例如：網路效能降低。由於蟲洞的出現會使網路拓撲產生變化，其兩端會吸引大量封包經由此通道傳輸，造成蟲洞及其附近節點的流量擁塞而嚴重延遲。這跟有線網路的概念一樣，封包大量出現時，這些節點必須將所有封包放入佇列中，當它們不再能即時轉送這些封包時，延遲時間會以次冪的方式成長；此外，當節點的暫存佇列溢位時，亦會發生封包遺失的問題，就產生了類似於阻斷服務攻擊的狀況，造成傳輸參數看似較佳，但等待時間卻反而更長的情況。

在下面的文章中，我們首先在第二章回顧幾種著名的蟲洞攻擊抵禦方法與協定，並說明其相關問題。接著在第三章中說明我們所提出的路由方法，以期能達到有效率的防範方案。最後，在第四章提出模擬與實驗的結果，來證實所提出的做法是正確的，並在第五章提出結論。

2.抵禦蟲洞攻擊的相關做法

2.1 視覺化蟲洞的方法

2004 年，Wang 等人[15]提出將網路拓樸視覺化的方法，把蟲洞顯示在拓樸上並加以分析。其做法大致如下：

步驟1. 將節點與節點間的距離以傳遞的時間差為參考，做非精確量測。

步驟2. 有一中央控制主機負責搜集各節點傳回的距離資訊，俟所有節點傳回資訊後，將其輸入一個 MDS-VOW (Multi-Dimensional Scaling - Visualization of Wormhole)機制。

步驟3. MDS-VOW 機制會輸出該網路的拓樸，如圖 2 所示，並建立每個節點的蟲洞指標，如圖 3 所示，並以此為判斷蟲洞的基準。

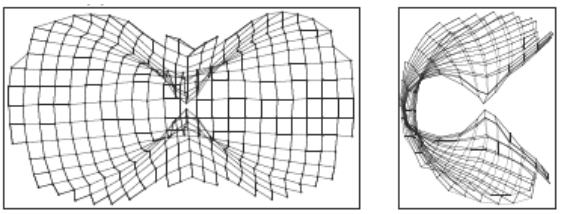

圖 2 具有蟲洞網路拓樸重建圖

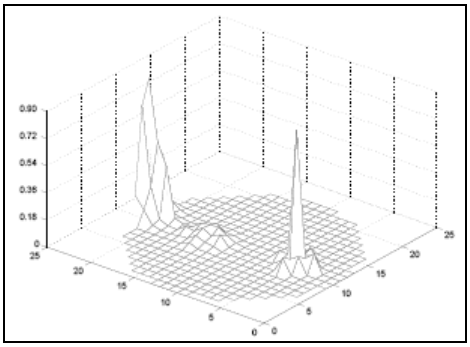

圖 3 蟲洞指標示意圖

我們可以看到，這個機制所建立的網路拓樸，直覺地顯示出蟲洞的存在與否。若在這個網路中沒有蟲洞存在，網路拓樸會相對地平坦，但會因誤差有些崎嶇；反之，若有蟲洞存在，則網路拓樸空間會被扭曲，如圖2。除了視覺化的部份之外，這個方法定義了一個蟲洞指標，在經過MDS-VOW計算出每個節點的蟲洞指標值後，即與預設的值做比較，若大於預設值者即視為蟲洞。

在其效能評估當中，在量測的誤差不要太大的狀況下，蟲洞的偵測率就可以達到很高。但是，由於這樣的機制採用了不精確的距離量測，故距離量測誤差加大的時候，容易產生誤判的狀況，如圖4所示，我們可以發現因錯誤導致的崎嶇特性已類似蟲洞產生扭曲的狀況。此時，該系統僅能偵測到70%的蟲洞，且誤報率接近10%。另外，對於非平坦的地形，或是對於兩個以上的蟲洞存在的狀況，也需要再做研究。

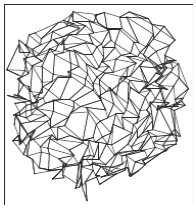

圖4 量測誤差大時的拓樸重建圖

除此之外，我們認為這樣的機制在確認距離較短的蟲洞上，會加深許多困難，尤其在其實驗中，都取了最邊緣的節點為例做探討，並不符合實際狀況。若蟲洞距離接近達到誤差會發生的範圍內，其偵測率應會比70%再降低許多，甚至無法偵測，且誤報機率也將提高許多。另外，由於搜集資訊量大，且其MDS-VOW機制在節點數n的狀況下，必須利用中央主機做到複雜度$O(n^3)$的運算，故以此方式計算蟲洞指標值效率不彰，並不甚實用。另一個問題在於，必須有一公正且運算快速的中央主機，但如此一來，與原本無線隨意網路沒有任何基礎建設的假定就不甚符合了。

2.2 封包控制的方法

2006年，Hu等人提出使用封包控制(packet leashes)[3]的方式來限制封包傳送的距離。作者提出了一個TIK protocol，由TESLA protocol[11]延伸而來，其意為TESLA with instant key disclosure。其協定假設時間必須精準地同步，並使用時間控制的

觀念，限制了封包傳輸的時間，也因此限制了封包傳輸的距離，此外再搭配上複雜的hash tree運算，來確保其時間的資訊不被攻擊者篡改，如此一來，收到封包的節點就可以確認封包傳送的距離是否符合傳送者的要求。

TIK協定主要分三大步驟如下：

步驟1. 傳送端初始化：傳送端用主密鑰產生 w 把次密鑰，並依固定的時間區間 I 依序給予次密鑰不同的有效期限。最後以所有次密鑰建立一 Markle hash tree，使得根端的 m 值可用以驗證所有葉端的次密鑰值是否正確。

步驟2. 接收端初始化：此協定假設所有接收端節點都知道傳送端的 hash tree 根 m 以及初始時間跟時間區間 I。此外，所有節點時間同步之最大誤差必須在 Δ 以內。

$S \rightarrow R$：$<HMAC_{Ki}(M), M, T, K_i>$

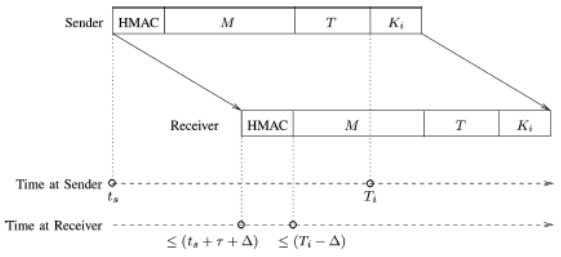

圖5 TIK協定中的封包傳送

步驟3. 傳送及驗證封包：參考圖 5，該協定封包含有四部份：HMAC、內文、驗證次密鑰K_i用的值T以及該封包使用的次密鑰K_i。傳送端傳送封包前，先預測接收端收完HMAC部份的時間t_r，並據此擇一次密鑰K_i使之t_r前有效，並在K_i到期時公佈其值。接收端收到HMAC後，先確認K_i仍有效，即未被傳送端公開。若K_i有效，則在收到封包尾端的K_i後，以m與T值驗證之，若K_i正確，代表時間在傳送端的要求內且未受竄改，最後就用此K_i驗證內文，若內文亦正確則接受此封包。

在這個協定中，用了很理想化的網路狀況來對抗蟲洞。首先，該協定必須依賴極精準的時間校正，但這在無線隨意網路中是相當困難的；此外，在傳輸時間上，該協定假設了蟲洞的傳輸較一般路徑慢，且一般節點間不得有任何延遲，故經由蟲洞的封包才會晚於有效時間，到達接收端被偵測出來，這些都是極不合理的狀況；最後，傳送者必須先知道接收者及中間路由節點的位置，才能預測到達的時間，這在無線隨意網路中若非經由一些特定的設備，也是不可能達成的，故我們認為這樣的協定在實用上的價值並不高。

2.3 其它方法

此外，還有許多抵禦無線隨意網路中蟲洞攻擊的文章被提出。例如[14]中，Song 等人提出 SAM 協定，這是基於 SMR 協定[5]改進而成的，透過資料的分析來判斷何者為蟲洞，但僅能適用於靜態的無線隨意網路環境；在[8]中，Lazos 等人提出以圖論的方式來監控蟲洞的方法，在其著作中，必須存在一種特殊的守衛節點(guards)，裝載定位的系統，並持續以大功率發送自己的位置，一般節點可以收到不同守衛節點發出的訊號，以判斷自己的位置是否合理，或可能遭受攻擊，但這樣的方式與無線隨意網路中沒有基礎建設的假定是相違背的，且此方法也僅適用於靜態的網路環境。另外，尚有如[1]中的 DelPHI 機制、或是[4]中的 Liteworp…等方法在近幾年被提出。

然而，在本章所提及的協定與方法大多需要特殊的假設與硬體設備，或是需要藉由非常大量的運算…等，才能偵測出蟲洞的位置以避免之。故我們希望能夠提供一個簡單又有效率的方法，來達到良好的防禦效果。

3. 提出抵禦蟲洞攻擊的新路由協定

現今的網路交易已成為一種方便快速的消費模式，然而也因此產生許多詐騙行為。對於預防詐騙，網路警察跟使用者都扮演了很重要的角色。網路警察的職責，必須在犯罪產生時，動用許多的資源，去追查出犯罪者，才能維護網路交易環境的安全；但對使用者來說，多一分警覺心，不輕易的匯款，不外洩重要資料，就能夠簡單地達到 99%的安全。本論文即以類似的概念，由使用者的角度出發，來設計一個抵禦蟲洞攻擊的新路由協定。

參考圖 6 為例來說明，在某個網路情境中，若大部份的路由都要經過大約 10 個跳躍數才能從起點端到達接收端，而某個路由路徑僅經過 3 個跳躍數就到達了接收端，則我們設計一個新的機制，略過這條可疑的路徑不去使用，就可以很容易地避免掉蟲洞的攻擊。

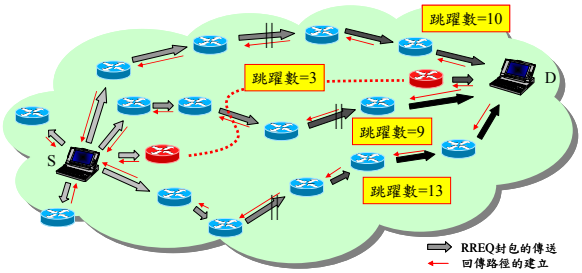

圖 6 跳躍數選擇示意圖

在本文所提出的新路由協定當中，參考了 RFC3561 的標準來設計路由的尋找與建力，其封包欄位定義如圖 7，其中圖 7(a)為 RREQ 封包、7(b)為 RREP 封包。起點端在有通訊需求時，會觸發一個路由尋找的程序如下：

步驟1. 將起點端位址、接收端位址及 RREQ ID 寫入該封包後，廣播該封包。

步驟2. 當任意節點收到此 RREQ 封包時，首先檢查起點端跟終點端的位址及 RREQ ID 以確認是否收過相同的 RREQ 封包。若收過則逕丟棄之，反之，若無收過相同的 RREQ 封包，則將本身位址加入該封包的中間點清單，再將跳躍數加一之後，重新廣播該 RREQ 封包。

經由一再的廣播 RREQ 封包之後，接收端將會收到這個 RREQ 封包。接收端收到後，會進行下列動作：會沿著 RREQ 傳來時建立的各路徑，逐一往來源端回覆 RREP 封包。

步驟1. 將起點端位址、接收端位址寫入該封包，並將跳躍數設為零。

步驟2. 加入一個路由的有效期限後，依照路由建立的各個路徑，往起點端回傳 RREP 封包。

步驟3. 中間節點第一次收到 RREP 封包時，將跳躍數加一，並將封包內各值暫存後，往下一節點傳送。

步驟4. 若中間節點收過相同起點端跟接收端的 RREP 封包，則將新封包中的跳躍數與暫存的跳躍數比較，若新值較原值小，則以新路由取代舊路由，反之則丟棄跳躍數較大的 RREP 封包。

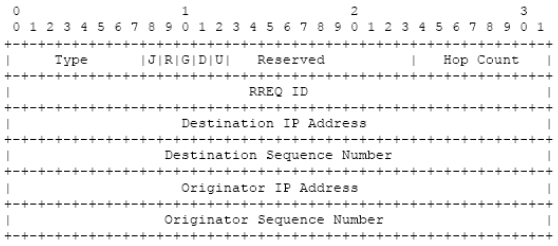

圖 7(a) RREQ 封包格式

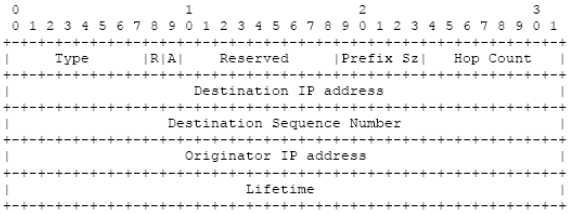

圖 7(b) RREP 封包格式

最後，回傳的 RREP 封包將會回到來源端，此時，以本文提出的機制判斷可用的路由。首先，

將所有收到的 RREP 封包中的跳躍數值取出分析，步驟如下：

步驟1. 將跳躍數值令為隨機變數X，則其累積分佈函數為$F_X(x)$。

步驟2. 取其累積分佈函數中的 a~b, 0<a<b<1 為安全區間，如圖 8。

步驟3. 取出安全區間對應的跳躍數值 i~j，並將該路由設定為合法路徑，其餘路徑則丟棄不用。

步驟4. 將合法路徑暫存在起點端，並由起點端通知接收端這些路徑後，就建立了一個雙向的路由。

步驟5. 起點端與接收端隨機地使用這些合法的路徑，如此一來，倘若蟲洞被篩選進這些合法路徑中，亦可降低其使用機率。

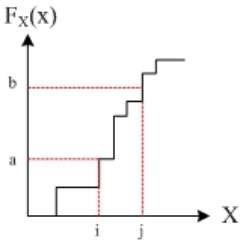

圖 8 安全區間對應示意圖

由圖 8 可以看出，設定完合法路徑後，起點端將不會使用一些過低跳躍數的路徑，而是選取看起來較為正常的路徑來進行通訊。如此一來，就可以利用這個簡單的方法，來避開蟲洞攻擊所佔據的路由。

但路由在使用的過程中，有可能中斷，所以在本文中也設計了一個維護路由的方法，來進行路由維持，可以分兩部份說明，首先是中間節點發現資料無法傳遞時的處理：

步驟1. 若中間節點無法傳遞資料，則視傳輸方向往回向起點端或接收端傳送一個 RERR 封包，內含有起點端位址、接收端位址及該路徑的中間點清單。

步驟2. 起點端或接收端收到 RERR 封包之後，將失效的路徑刪除後，將此訊息透過其他可用的路徑通知對方。

步驟3. 當可用路徑皆隨時間中斷後，起點端就必須重做路由尋找及建立的動作。

除了中斷後由中間點告知路由的兩端，起點端本身也會做路由的維持。在本文提出的路由協定中，對每一條路由設定了有效期限，在有效期限將屆時，若起點端已不須使用該路由，則刪除相關資訊；反之，若該路由仍有資料在傳送，則起點端將採取類似主動式路由協定的方式來維持已知的路由。其步驟如下：

步驟1. 起點端會循所有可用的路由路徑觸發一個單一路徑傳播的確認封包 RCHK，內含起點端位址、接收端位址及該路徑的中間點清單，以確認路由是否依舊正常維持。

步驟2. 接收端收到該封包，將加上一個新的路由期限，並依原路徑回應已收到確認訊息 RACK。

步驟3. 中間點收到 RACK 訊息時，更新其路由有效期限。

如此一來，起點端就不用大費周章地再做一次路由尋找及建立的動作，也可以省去重新篩選路由的過程。

4.模擬與實驗

對於本文所提出的新路由協定，我們使用了一個 C 語言撰寫的程式來模擬路由建立的過程。此程式為事件驅動(event-driven)的程式，會依照時間先後，安排在路由請求的過程中所有的事件，這些事件包含：

(1) 以亂數安排所有節點的位置；

(2) 起點端發送 RREQ 封包；

(3) 路由在空中傳遞的時間；

(4) 每個節點間有亂數的延遲時間；

(5) 接收端傳回 RREQ 時，中間點選擇路徑的方式；

(6) 起點端收到所有路徑後的篩選動作。

在本實驗中採用的模擬環境參數設定如下：

(1) 節點數：300；

(2) 環境大小：1000m x 1000m；

(3) 傳輸距離：200m；

(4) 節點延遲：0.02~0.05ms；

(5) 模擬次數 100 次；

(6) 節點隨機佈設，但起點端為(200, 200)，接收端在(800, 800)，而蟲洞兩端則在(350, 350)與(650, 650)。

我們進行了實驗(a)與實驗(b)來說明本文所提出的新路由協定避開蟲洞的效果。由圖 9(a)與圖 9(b)分別可以看到篩選完的結果。

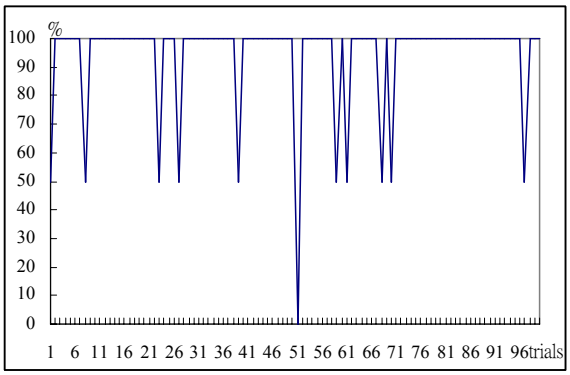

圖 9(a) 取分佈中間 1/3 為合法路徑之結果

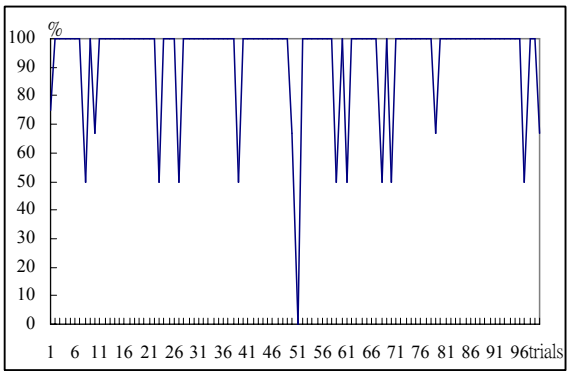

圖 9(b) 取分佈中間 1/2 為合法路徑之結果

以下分別說明兩個實驗的結果：

實驗(a)：參考圖 9(a)，本次實驗取累積分佈函數的中間 1/3 為合法路徑，亦即取 a=0.333、b=0.667 的情況。從圖中可以看到在 100 次的實驗當中，僅有數次在篩選的過程中選到蟲洞的路徑。最後，可以得到所有實驗的平均成功率約為 94%。然而，例如在第 51 次實驗中，除了經過蟲洞的路徑外，由於隨機的佈點，故並沒有其它路由能被建立，篩選的結果無法避免；其餘有落差的實驗也跟路徑數較少有關。

實驗(b)：參考圖 9(b)，我們以相同的實驗資料，採用較寬鬆的篩選規則，也就是取累積分佈函數的中間 1/2，a=0.25、b=0.75 為合法路由的狀況。其結果與 9(a)相去不遠，但因篩選較為寬鬆，故有較多次蟲洞被設為合法路徑的情形產生。在此次實驗中避免使用到蟲洞路徑的總平均成功率約為 92.917%。

一般來說經由蟲洞的路由，跳躍數會較正常路由來得小，因此可以發現實驗結果對於篩選的區間敏感度並不是很大，因為最小的幾個值大多會被排除在選取的範圍之外。

另外，分析實驗中路由的平均跳躍數，可以得到未經過本協定篩選的所有 232 條路徑，其平均跳躍數約為 4.81 個；在(a)實驗中，所有 154 個被篩選為合法路徑者，其平均跳躍數約為 4.773 個；而在(b)實驗中，所有 212 個被篩選為合法路徑的平均跳躍數則約為 4.788 個。從比較可以得知，經由本協定篩選過後的路由，其平均跳躍數較未篩選前更低。這是因為在本協定中被篩選為合法路徑者，皆在累積分佈函數的中間區塊，故過低或過高的跳躍數都同時被濾除了，使得平均來說，傳輸的效能更為理想。

5.結論

自從蟲洞攻擊的問題在無線隨意網路的研究受到重視以來，已有許多的學者提出相關的著作試圖解決此問題。如第二章所討論的：Wang 等人採用中央主機加上 MDS-VOW 機制，做大量的拓樸運算；Hu 等人則利用大量的 hash 運算來做封包控制的安全認證，然而其假設的網路環境是不合實際的；其餘如圖論的方法…等，皆需要在網路中置入特殊的硬體或假設，雖然這些方法大多具有良好抵禦蟲洞的能力，但實用性上卻有待商榷。故本文提出一個不需要任何特殊假設及硬體設備的新路由協定，藉著路由資訊的搜集及其跳躍數之分析，就可以很實際的避開絕大部份的蟲洞攻擊。此外，從實驗上也可以證明本文所提出的新協定不需任何特殊機制就可以達到 90%以上的成功率，且因為運算量極小，對節點的負擔並不大。綜合以上，本路由協定是一個良好的抵禦蟲洞攻擊之新協定。

誌謝

本研究承蒙國科會「資通安全人才培育計畫-人才培育」之補助，計畫編號為 NSC-94-3114-P-006-001-Y，特此致謝。

參考文獻

[1]. H. S. Chiu, K. S. Lui. “DelPHI: Wormhole Detection Mechanism for Ad Hoc Wireless Networks” in IEEE ISWPC 2006, Pages 1-6, Jan. 2006

[2]. S. Corson, J. Macker, “Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations”, in IETF RFC 2501, Jan 1999

[3]. Y. C. Hu, A. Perrig, D. B. Johnson, “Wormhole Attacks in Wireless Networks” in IEEE Journal on Selected Areas in Communications, Vol. 24, No. 2, Pages 370-380, February 2006

[4]. I. Khalil, S. Bagchi, N. B. Shroff. “LITEWORP: a lightweight countermeasure for the wormhole attack in multihop wireless networks” in IEEE DSN’05, pages 1-10, June 28 – July 1, 2005

[5]. A. Perrig, R. Canetti, D. Tygar, and D. Song, “Efficient authentication and signature of multicast streams over lossy channels”, in Proc. IEEE Symp. Res. Security and Privacy, pp. 56–73, May 2000

[6]. Z. Li and Y. K. Kwok. “A New Multipath Routing Approach to Enhancing TCP Security in Ad Hoc Wireless Networks” in IEEE ICPPW’05, 2005

[7]. L. Lazos and R. Poovendran, “SeRLoc: Secure Range-Independent Localization for Wireless Sensor Networks”, in ACM WiSE’04, October 2004

[8]. L. Lazos, R. Poovendran, C. Meadows, P. Syverson, L. W. Chang. “Preventing Wormhole Attacks on Wireless Ad Hoc Networks: A Graph Theoretic Approach” in IEEE WCNC 2005, Pages 1193-1199, 2005

[9]. A. Maltz, J. Borch, J. Jetcheva, and D. B. Johnson, “The Effects of On-Demand Behavior in Routing Protocols for Multihop Wireless Ad Hoc Netwroks,” IEEE J. Selected Areas in Communications, vol. 17, no. 8, pp. 1439–1453, Aug. 1999

[10]. C. Perkins, E. Belding-Royer, “Ad hoc On-Demand Distance Vector (AODV) Routing”, in IETF RFC 3561, July 2003

[11]. S. Lee and M. Gerla, “Split Multipath Routing with Maximally Disjoint Paths

in Ad Hoc Networks", Proc. of IEEE ICC, Vol.10, pp.3201-3205, May 2001

[12]. A. Perrig, R. Canetti, D. Tygar, and D. Song, "Efficient authentication and signature of multicast streams over lossy channels," in Proc. IEEE Symp. Res. Security and Privacy, pp. 56–73, May 2000

[13]. L. Qian, N. Song, X. Li. "Detecting and Locating Wormhole Attacks in Wireless Ad Hoc Networks through Statistical Analysis of Multi-path" in IEEE WCNC 2005, Pages 2106-2111, 2005

[14]. N. Song, L. Qian, X. Li, "Wormhole Attacks Detection in Wireless Ad Hoc Networks: A Statistical Analysis Approach", in IEEE IPDPS'05, 2005

[15]. W. Wang, B. Bhargava. "Visualization of Wormholes in Sensor Networks" in ACM WiSE'04, October 2004

[16]. M.G. Zapata, "Secure Ad hoc On-Demand Distance Vector (SAODV) Routing" in IETF Internet Draft, draft-guerrero-manet-saodv-06.txt