追蹤無線網路匿名移動癱瘓服務攻擊者感測網路

楊明豪,李軒豪,廖柏穎,胡弘淵,李國瑋
中原大學 資訊工程系
mhyang@cycu.edu.tw

摘 要

針對惡意攻擊者於無線網路端發動癱瘓服務式攻擊,當其攻擊封包經由無線隨意網路來攻擊網際網路上之伺服器時,由於該攻擊者不需至受害者端回收資訊,其 IP 位置極可能假造,因此遏止該項攻擊可經由追蹤無線網路攻擊位置來源,再進一步來限制被定位之攻擊者之頻寬,以防止其繼續進行癱瘓服務攻擊。然而,因為行動裝置的移動性使的攻擊者和無線網路之中繼路由器可能因變換位置,以及中繼路由器為一般電腦容易遭受攻擊而成為跳板的特性,使的原有之有線網路上所發展之追蹤技術無法應用於無線隨意網路。

在本論文中,我們使用 nRF24E1[9]晶片來實作模擬追蹤無線區域網路之匿名攻擊者,我們參考楊所提之追蹤無線移動攻擊者論文[7],將其被動的只有於 AP 蒐集各利用 DSR 繞境至 AP 之移動裝置來追蹤移動攻擊者,改為主動的利用於網路中佈置感測器來追蹤於無線網路中發動攻擊之移動匿名者。因此,我們利用 24E1 晶片之 2K 位元組 code segment 實作無線隨意網路中之攻擊追蹤感測器且實作 Dynamic Source Routing(DSR)[5]此協定於該晶片上以建立路由將資訊透過無線網路傳回後端資料庫,以在無線網路上實作追蹤該網路內發動匿名攻擊的攻擊者位置。此外,我們將利用個人電腦模擬基地台來儲存封包紀錄且在此利用楊所提之追蹤演算法來計算當時網路拓撲,所以我們將在 AP 端以個人電腦來接收無線感測器回傳之封包,並在此分析無線網路傳送之封包,藉以用來追蹤攻擊者可能出現之位置。

一. 前言

隨著網路科技的快速發展,以及應用軟體使用界面的簡單化、人性化,網路使用人口正迅速膨脹。另一方面因為電腦的普及化,為了因應各種不同類型使用者以及寬頻的傳輸環境,使得網路上傳輸的檔案格式越來越多元化,並且有著各式各樣的應用程式以提供更多、更好的服務。此外,這幾年瀏覽器的興起,更帶動了電子商務的熱潮,使得網路上所儲存或是在網路上傳輸的資訊越來越具有價值。再加上因為網際網路的便利性,許多人會將重要資料放置在網路上,以方便檔案可以和他人分享,或是自己可以在任意地點處理公事。然而,在如此多樣的應用程式協定(Telnet, FTP, HTTP, SNMP, POP, NetBIOS…等) 以及各型各色網路使用者的情況下,使得網路傳輸的管理和控制越來越困難。

相對於直接對受害者端的漏洞發動攻擊之明顯特徵,阻斷服務攻擊(DoS)[1]和分散式阻斷服務攻擊(DDoS)[1]其攻擊封包內容本身沒有明顯特徵。被攻擊網路伺服器的使用者僅感受到明顯的網路延遲、大量的封包遺失,或根本無法與伺服器建立網路連線,攻擊者據此已可輕易達到其阻斷服務之效果[1]。另一方面,許多 DoS 攻擊程式都能相當容易透過網路取得,因此現在的駭客並不需要有高超的技術或者知識就可發動癱瘓服務攻擊,這也使得網路攻擊事件變得更加地泛濫。

相對於眾多網路攻擊事件中,分散式阻斷攻擊成了最引人注目的焦點。根據 CSI/FBI 2006 的調查報告[6]顯示,本年度回覆 FBI 調查的單位有 25% 於今年遭受過 DoS 攻擊。DoS 攻擊已經成為所有攻擊類型發生比例最多的第五名,且這類攻擊對企業造成的損失金額為所有攻擊類型之第五位,這足以顯示 DoS 攻擊對目前資訊安全傷害之嚴重性。另外依據 CSI/FBI 歷年的網路犯罪與安全報告顯示,DoS 攻擊所造成之影響有逐年上升之趨勢。我們更於其中內容發現,雖然目前 DoS 對該單位傷害很嚴重,但是所有單位均無法針對該類攻擊提出有效之防護方法。

當受害者遭受到網路之大規模攻擊阻斷服務攻擊時,由於攻擊者並不期待從被攻擊者電腦中取得資訊,因此經常會使用假造之 IP 來對受害者發動攻擊,藉以掩飾自己的身分,而且由於路由器爲追求快速繞境至目的地,路由器只會檢查封包之目的地即將封包送至所對應之通道,因此攻擊者便有機會可以利用大量假冒之 IP 對受害者端發動攻擊以造成被功擊者端因此服務癱瘓不能正常運作,且無法由攻擊封包中判斷攻擊來源為何。

目前有線網路上對於追蹤攻擊者由何處發動攻擊除了有利用 TTL 值差異外,還有利用受害者電腦中之連線是否有異常 IP 流入等方法,而這些是不需要路由器配合,這些方法都需要知道正常範圍資訊且較容易判斷錯誤,所以大部分的方法都需要路由器配合來將路由器本身之特殊辨識碼,如 IP 紀錄於原來封包上(DPM[2], PPM[8],[13])、另外發 ICMP 封包來通知被害者端(I-Trace[11])、或者紀錄於路由器所附之另外儲存空間等方法。

記錄攻擊封包路徑研究方法可以主要分成三大類,packet marking、packet logging 和 messaging。接下來我們將探討目前利用這三種標記方法之追蹤方法。

Packet Marking

封包經過路由器時，路由器會將自己的 IP 位置記錄在經過的封包內。這封包所附追蹤資訊，會隨封包到達目的端後儲存在目的端的記憶空間。當攻擊發生後，利用這些儲存於目的端的資訊來回復原來的攻擊路徑。當路由器在傳送封包之前，它會將路徑資訊放入封包中，再進行傳送。因此，封包的原始位置即可用路徑資訊找出。

Messaging

當封包經過合作的路由器，該路由器會以其它封包(ICMP)紀錄該封包經過的路徑。這些留有紀錄的封包會和原來的封包一起送到目的端儲存，當攻擊發生時可將攻擊封包和這些紀錄路徑封包一起追蹤攻擊來源。封包路徑是放入 ICMP 封包中，其中包括轉送的路由器以及其他相關的資訊。

Messaging 封包追蹤攻擊位置的技術[3]，[11]，當攻擊者發動攻擊時，其所發出的封包經過配合的路由器，該路由器即會發出相對於該封包的 ICPM 封包至其封包所欲到達之目的地。因此，一個攻擊封包會對應到數個 ICMP 封包，至於其所對應的個數量，則取決於該攻擊封包所經過配合路由器的數量。然而，這樣的做法有一致命的缺點，就是其所發出的 ICMP 封包數量是數倍於原始攻擊封包。也就是說一但攻擊者利用該項特性發動 DoS 攻擊，則攻擊者只要花費原來攻擊的數分之一的力氣，即可以癱瘓其攻擊目標之網路頻寬及電腦。為節省追蹤攻擊者所產生的封包數[10]，可以結合 Packet logging 和 Messaging 使得發出封包的數量可以減少，也可減少路由器儲存封包資料的空間。

Packet Logging

Packet Logging 的方法會將經過的封包資訊，紀錄在經過的路由器儲存空間內。當攻擊發生後，目的端會詢問所有路由器經過封包的資訊，以重建原有的攻擊路徑。而這種技術是利用查看 log 的追蹤技術，網路中的路由器會將儲存轉送的 IP 封包記錄於 log 中，藉此找出攻擊的路徑。T. BaBa 就是利用此種方式來找出攻擊封包的整個路徑，但這種方式會十分耗費儲存空間。因此，SPIE[12]採用 Bloom filters 來儲存決定性的封包摘要(digest)。另外，Hash based (bloom filter) [3]，[4]，[10]也是以單一封包來追蹤攻擊者。當攻擊者發動攻擊，其所發出的封包經過配合的路由器，該路由器會將傳輸中之攻擊封包表頭（Packet header）裡面的不變欄位雜湊（Hash）成一個 Digest。

然後，將其 Digest 儲存於路由器本身另外附加之記憶體，並將其對應至路由器中之表格。一但受害者端遭受到攻擊時，受害者端會將其攻擊封包所對應之 Digest 廣播至網際網路。而路由器接收到該封包，會查詢該 Digest 是否存在於該路由器內，並將其查詢結果回傳給受害者。受害者便可以基於所有路由器回傳之資料，建構出攻擊者之攻擊路徑。雖然如此 Packet Logging 的方法並非完善，它存在著下列幾個問題。首先，因為路由器的儲存空間有限，所以一但其儲存空間飽和，其相對應之攻擊路徑資訊就會消失，即會影響其追蹤攻擊者的能力；再者，由於其對應方法乃是利用 Hash 值，會有 Collision 的情況產生而誤判攻擊路徑；另外，各路由器必須在其上增加數百萬位元組記憶空間，實屬不太實際；最後，以路由器去尋找一封包相對應的位元是否存在，這項工程相對於路由器本身的處理能力實在太過於沉重。綜上所述，以及 Core Router 一天經過的封包數量實在過於龐大，我們可以看出要以路由器紀錄所流經封包來追蹤攻擊者實在不是一件簡單的事情。

然而這些方法均無法針對追蹤無線使用者，因為之前所有方法中最好的也只能找到最接近攻擊者之路由器，且目前國內外之追蹤攻擊研究大部分都不考慮攻擊者會移動之特性及無線隨意網路之路由器本身易遭受攻擊之特性。當攻擊發生來源端是由無線網路時則無法追蹤正確無線網路內之攻擊來源。

二.追蹤無線匿名攻擊者文獻回顧

因無線網路設備增加和無線頻寬的需求增加，使攻擊者具有利用行動設備自無線網路發出癱瘓式服務攻擊之能力。然而無線網路環境具有資源缺乏的特性，如行動設備能源的不足和路由協定需發送大量封包來建立連線。在無線隨意網路中行動設備必須擔任網際網路的路由器角色來建立路由表，且因為一般行動設備都只是一般的個人電腦，且這些個人電腦具有移動性，一但這些電腦移動後，所有路由器所標記的資訊很有可能就會找不到攻擊中繼點而造成我們沒有辦法追蹤攻擊者。此外，一般的個人電腦由於服務通常開放的比路由器多，使用的作業系統漏洞也較多，再加上使用者習慣不良的話，個人電腦相對於路由器被惡意攻擊者攻陷的機率也相對於一般路由器高出很多，也因此中介點路由器之路徑記錄有可能因為成為攻擊者之跳板而不正確。因此目前於有線環境所發展之追蹤法均無法於無線環境中追蹤攻擊者。

Huang 和 Lee 提出於無線隨意網路(ad-hoc network)之追蹤攻擊者方法--熱區追蹤法 (hotspot traceback) [14]來追蹤無線網路端之癱瘓服務攻擊者。Huang 和 Lee 認為有線網路追蹤和無線網路追蹤最大差異為無線設備之移動性和無線中繼路由器可能遭受攻擊而成為跳板。因此改良原有之有線追蹤法 I-trace[11]，並加入攻擊者會移動以及中間點路由有可能遭受攻擊的特性而發展出無線隨意網路熱區追蹤方法。該方法改變原有 I-trace 使用之 bloom filter[4]來成為 TBF(Tagged Bloom Filter)，來記錄無線網路內任意兩個節點可能的相對距離。此

追蹤法在隨意網路(ad-hoc network)架構下可以加入攻擊者以及路由器具有移動的特性，利用 TBF 儲存所有經過該路由設備封包相關的欄位和 RTTL(Relative Time to Live)並配合所建立之鄰接串列(Neighbor List)的幫助建立攻擊路徑圖。藉分析無線隨意網路攻擊路徑圖找尋攻擊者可能位於無線網路之所在範圍而找出攻擊者可能存在於無線環境中之熱區。

Huang[14]所提出之演算法雖然可以追蹤無線攻擊者至一可能發動攻擊之區域，但是其最後鎖定可能攻擊範圍過於廣大，且 hotspot traceback 沒有分析不同時間傳送至該無線網路攻擊警告可能為同一攻擊者因移動所造成之現象，對於追蹤實體攻擊位置會因為可能攻擊者太多而造成相當大的困擾，因此揚提出 WiTrack[7]來增加追蹤的精準度和合併因移動而造成之攻擊地點轉換。WiTrack 假設若攻擊者之無線隨意網路繞境是依照 DSR 演算法傳輸的封包至 AP 並對網際網路之伺服器發動癱瘓服務攻擊，則 AP 會將傳輸所經過 AP 之所有節點之封包路徑記錄於 AP，並利用時間戳記標示存於 RGH Table(Routing Graph History Table)裡面所有無線隨意網路拓樸之變化，當偵測到遭受到攻擊時，會先看檢查該封包是否曾出現於 RGH Table 內，若有才表示次攻擊節點在此攻擊拓撲裡，再來利用這個時刻的攻擊路徑以及之前所建立出攻擊當時之的攻擊網路圖 AG(Attack Graph)，以追蹤攻擊當時之攻擊者於無線隨意網路內之位置，另外，會將前一次之攻擊拓撲圖 AG 與此次攻擊路徑相比對，若兩次攻擊警告拓撲合併計算後可能由上一次攻擊地點移動至下一個攻擊地點，由於該網路拓撲所有變化都因為時間戳記之不同而被標示，所以合併攻擊圖時可以依照時間戳記來判斷網路拓撲之變化，因此 WiTrack[7]可以判斷不同 IP 的攻擊者是否可能為同一人。

追蹤匿名攻擊者系統

由於有線網路追蹤技術相較追蹤無線網路上具移動特性攻擊者研究成熟很多，因此目前已有國外研究計畫實作 Source Path Isolation Engine (SPIE)[12]這種於 IP 層上追蹤攻擊者的系統，該系統在路由器上利用另外儲存設備以 Hash based 的機制將來源端經過該路由器之封包資訊儲存記錄下來以便於追蹤。紀錄的資訊有封包目的地和此封包估計到達目的端的時間，當受害者因網路流量異常或是封包要求使用過多 Memory 需要查詢攻擊來源時，將檢查之前所儲存的封包資訊。而網路流量檢查機制則依據 router 計算和儲存的封包資訊。SPIE 提供 router 作封包彙整及允許 router 追蹤封包。受害者因此可向路由器詢問攻擊封包是否經過此路由器，而藉此繪製出攻擊的路徑進而找出攻擊者。

SPIE 系統是由網路上元件以分層架構組成，封包檢查機制(DGA)、追蹤機制(SCAR)、和路徑重建(STM)三個主要元件所負責:,

1 Data Generation Agent (DGA) : DGA 將流經它的封包資訊整理後儲存在 Digest Table 中，紀錄的資訊有封包目的地和此封包估計到達目的端的時間，而從這些表格中可整理出指定之時間區間內在此區域中封包流動情形。DGA 有兩種形式，第一種是更改 router 核心使其擁有 SPIE 所具有之功能，另一種以 Box 形式置放在網路中，負責記錄一個或多個實體 router 的網路資訊。
2 SPIE Traceback Manager (STM)： 為 SPIE 追蹤的中央設備，STM 負責建置出攻擊圖形，同時也負責 Security 部分。
3 SPIE Collection and Reduction Agent (SCAR) : SCAR 負責一部份特定區塊，接收屬於負責範圍內 DGA 所獲取的封包資訊並建立負責區域內的子攻擊圖形。

雖然 SPIE 在攻擊者進行攻擊和被害者端 IDS 通知該路由器追蹤攻擊者時間間隔短暫的情況下可以成功的追蹤攻擊者經過之路由器。然而，SPIE 並不具有追蹤具有移動性質的攻擊者的能力，一但攻擊者於攻擊中移動位置，SPIE 會將其辨識為兩個不同來源的攻擊者，對於追蹤攻擊者方面來說，會於一次測試中產生太多的攻擊者，而造成後續處理如停止攻擊的困難性。另外，該系統所基於之方法並無法解決負責追蹤之中間點遭受攻擊而變成跳板的問題。

不同於有線網路之攻擊，無線設備具有相對較高的移動性，因此在無線網路中追蹤攻擊來源之方法顯得更為重要，然而就以無線隨意網路為例，我們要追蹤攻擊來源必須考慮攻擊者之移動性。我們參考楊所提之追蹤無線移動攻擊者方法 WiTrack[7]，將其被動的只有於 AP 蒐集各利用 DSR 繞境至 AP 之移動裝置來追蹤移動攻擊者，改為主動的利用於網路中佈置感測器來追蹤於無線網路中發動攻擊之移動匿名者。因此我們設計並實作一個可以應用於追蹤在無線區域網路內攻擊者之感測器，我們提出的方法利用感測器記錄攻擊者所傳送之封包，並且將所紀錄之資訊從無線網路透過 DSR 傳送至 Access Point 以作為將來追蹤攻擊者使用。此外，該 AP 為有線網路端和所監控無線網路端間之閘道器，監控利用該被監控無線網路穿過網際網路攻擊於其他無線網路或有線網路伺服器之攻擊封包。

本論文的目的為利用 nR24E1 實作追蹤攻擊感測器，並於 AP 端實作楊[7]所提之追蹤無線移動攻擊者方法，以重建感測到攻擊封包之感測器網路拓撲，在 IDS 通知攻擊封包特徵後可以追蹤在無線網路內以匿名方式發動癱瘓服務式攻擊之攻擊

者。由於駭客的攻擊十分猖獗，如果我們能夠舉證出攻擊的證據，並且準確、快速地找出真正的入侵者，才能有效的嚇阻攻擊事件的發生。由於我們於無線區域網路中佈置大量的感測器來追蹤於無線網路中發動攻擊之匿名者，因此我們預計使用內含8051CPU (最大20MHz)與Radio Transceiver的硬體裝置[9]，且其記憶體容量為4K bytes之nRF24E1晶片來實作模擬追蹤無線網路匿名攻擊者之感測器，因為該設備成本較為低廉且已經包含基本的無線網路傳輸功能，具有TCP之protocol stack，對於我們在這晶片上實作 DSR 協定沒有太大的阻礙。

我們將利用個人電腦來擔任無線網路與有線網路之閘道器，用以儲存封包紀錄且要負責計算當時網路拓撲，所以我們將在AP端以個人電腦來接收無線網路封包，並利用 WiTrack[7]分析無線網路傳送之封包來追蹤攻擊者可能之位置。因此，即使駭客從無線網路內對網際網路之伺服器發動癱瘓式服務攻擊，我們仍然能夠追蹤到攻擊封包的原始發出位址，以嚇阻 DDoS 攻擊，並且進一步的辨識因為攻擊者在攻擊同時移動而從不同時間、不同位置發動之攻擊為同一個攻擊者所發動之攻擊，以減少攻擊警告數量，因為一但發現癱瘓式服務攻擊，一定伴隨著大量的攻擊封包，若無法辨識這些不同時間從不同位置所發送之攻擊封包可能為同一攻擊者移動後所產生的來減少攻擊警告數量，那會使的攻擊之追查因為數量太大而變的不可行。因此，我們必須要將移動中之同一攻擊者警報節點合併，以確保追蹤資訊之功用。

三. 感測網路追蹤無線攻擊者方法

楊所提之追蹤無線移動攻擊者方法 WiTrack[7]，只有被動的於 AP 蒐集各利用 DSR 繞境至 AP 之移動裝置所送封包來追蹤移動攻擊者，且無線隨意網路節點可能不是利用 DSR 將封包送至 AP 而是利用 AODV 或是其他繞境演算法將封包由節點送至 AP。如此一來，WiTrack 就無法追蹤於無線網路發動癱瘓服務攻擊之攻擊者位置。因此，我們將 WiTrack 改為主動的利用於網路中佈置感測器來追蹤於無線網路中發動攻擊之移動匿名者。利用佈置之感測器來記錄所有經過之封包，並將封包流動紀錄於 AP，待追蹤到感測到攻擊封包之感測器，可以利用定位的技術來找出攻擊之實際位置。不過定位的問題不在本篇論文討論的範圍，我們可以利用定位技術[15][16][17]來找出攻擊者當時所在實際位置。在此，我們除了修改 WiTrack，使其演算法可以改為利用感測器來蒐集封包。另外，爲了在無線網路找出一套有效的追蹤無線匿名攻擊者位置之方法，建置出一個能夠模擬無線網路的環境與攻擊者的位置來實驗我們的追蹤理論，我們使用 nRF24E1[9]晶片實作無線網路節點，並且用來模擬實際的無線網路環境。另外，實作 Dynamic Source Routing(DSR)[5]演算法來建立出整個無線網路的傳輸路徑，利用我們會產生並紀錄下每一個時間點的網路拓撲，並利用演算法分析每一個時間點的拓撲進而找出攻擊者的所在位置。我們所設計之無線感測網路整體架構圖 1 所示，所有感測由無線網路傳輸至 AP 之攻擊封包器會以 DSR 繞境到 Sink node 並以 RS232 連到後端資料庫進行分析。

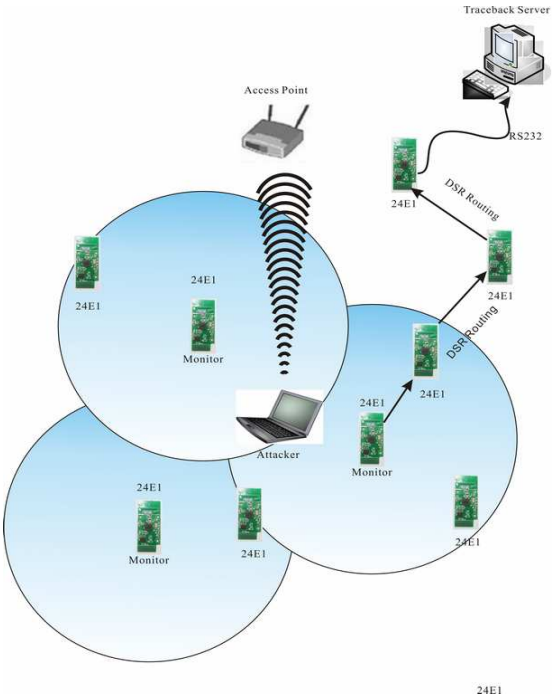

圖 1：無線追蹤感測網路架構圖

我們利用 nRF24E1 晶片實作出無線感測節點，當攻擊者於無線網路發動攻擊，監測範圍內之感測器會監測攻擊者所傳送之封包，並將所監測到之封包內容利用如圖 2 的 Packet Logging 方法來記錄攻擊封包以追蹤匿名攻擊者。

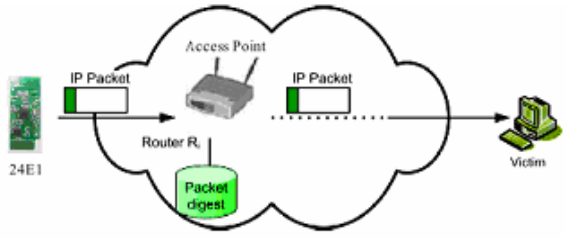

圖 2：攻擊封包記錄機制

我們所提出之感測網路追蹤機制分成三個階段，第一階段為封包記錄階段，第二階段為收到受害者端一個攻擊提示所啟動之追蹤攻擊和攻擊拓撲重建，第三階段為收到多個攻擊追蹤警告後所啟動之移動攻擊拓撲圖合併階段以減少多餘之攻擊提示。

第一階段即是在一般狀況下，所有的感測器會

將經過的所有封包資訊，利用 Packet Logging 紀錄在經過的路由器儲存空間內。當攻擊發生後，目的端會詢問所有路由器經過封包的資訊，以重建原有的攻擊路徑。

當一個感測器感測到傳往 AP 封包時，該感測器會進行下列幾個步驟：

1. 截取該封包之部分不變欄位製作雜湊值
2. 將該雜湊值利用 DSR 傳往後端資料庫
3. 資料庫截取該封包紀錄該雜湊值以及感測器之送往資料庫之 DSR 繞境路徑資料庫於如表 1 之 RGH 表
4. 若該 DSR 路徑不同或感測器 IP 是新的則時間戳記是否要增加

在第一步我們跟採用 Bloom filters 的技術來儲存封包中具有決定性的摘要(digest)以節省儲存空間。當攻擊者發動攻擊，其所發出的封包經過配合的路由器時，該路由器會將傳輸中之攻擊封包表頭（Packet header）裡面的不變欄位如圖 3 IP 表頭內之白色欄位，雜湊（Hash）成一個 Digest 再紀錄下來。

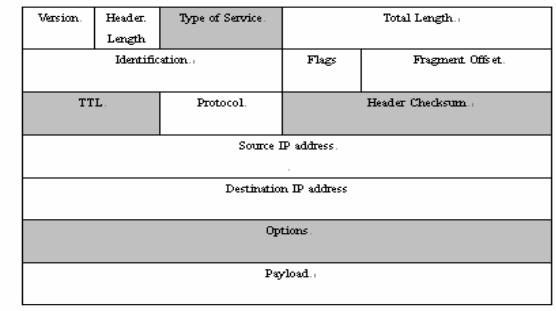

圖 3：封包表格內擷取來做雜湊之不變欄位

第二步則是將封包利用 DSR 建立傳輸路徑，將雜湊結果於利用感測器之間傳輸至後端資料庫，藉由數個感測器把封包從一個感測器傳送到另外一個感測器。每個感測器都會遵守 DSR 的規範來接收及發送封包，以維持封包傳遞的正確性。當一個感測器收到封包時，它會先去檢查此封包的 CRC 是否正確，如果正確則接收進來並且儲存在感測器記憶體裡的 data 部分，否則會將此封包丟棄。當封包被儲存到感測器記憶體後，我們將會去判斷此封包表頭的 type 是屬於 DSR 裡的那一個，然後去做其相對應的功能，例如 Route Discovery 裡的 REQUEST、REPLY 跟 SOURCEROUTE 等，使得封包能夠順利的繼續往下傳遞，直到成功送達目的地為止。

當後端伺服器收到封包時，我們可以從收到封包之 DSR 表頭的 source route 裡，獲得感測器送出封包的所有路由資訊。我們會將新獲得的路由資訊和來源 IP 和資料庫之 RGH 表做比對，若這是一個新的來源 IP 表示該封包是由新的節點發出，若是該新獲得路由路徑和相同來源 IP 之最近更新路徑不同，表示該封包由來源點送至後端伺服器和前一次該節點送至該伺服器所經過之網路拓撲不同，也就是經過之網路可能有節點移動，所以這兩個情況我們都會將時間戳記加一。在後端伺服器之資料庫中我們用如表 1 之 RGH(Route Graph History) 去記錄網路拓撲的變動，我們可藉此找到發生攻擊當時無線網路的拓撲圖。

表 1： AP 所儲存之 RGH 範例

Node / Time	N_1	N_2	N_3
T_1	$P(N_1,R_1)$		
T_2		$P(N_2,R_2)$	
T_3		$P(N_2,R_2)$	$P(N_3,R_3)$
T_4	$P(N_1,R_4)$	$P(N_2,R_2)$	$P(N_3,R_3)$

RGH 表內會存每一個時間點、每個節點的路徑，當偵測到節點有新的路徑時，會在 RGH 表內建立一個新的時間戳記並紀錄新的路徑以及感測器所記錄之封包雜湊值。由於 DSR 表頭裡包含封包的時間戳記和攻擊者的來源 IP 位址，而且接收端在收到封包後需要將資料保留在記憶體中一小段時間。第一欄為表頭摘要資訊用來連結該表第二欄資訊和原始封包，第二欄為時間戳記和原來封包之來源路由。所以我們可以搜尋此表頭摘要表來找出攻擊當時之時間和攻擊當時此封包在無線網路經過之感測器。

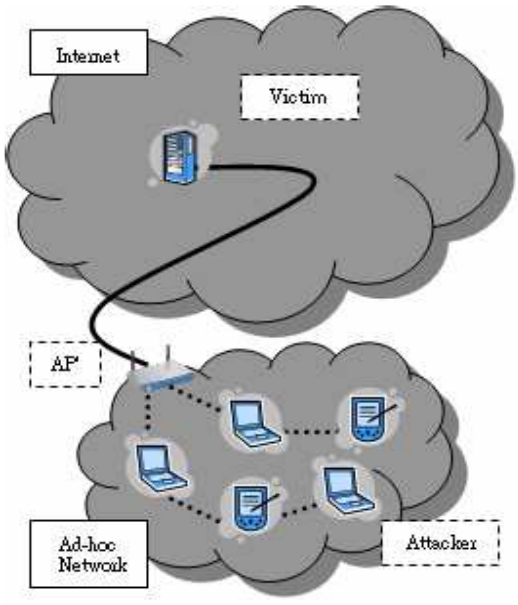

圖 4：無線攻擊環境架構示意圖

第二階段即當攻擊發生後，受害者端之 IDS 會利用有線追蹤機制追蹤到發動攻擊之無線路由器(AP)，因為無線網路的節點如圖 4 可能隨時都在移動，因此當攻擊被偵測到時與攻擊發生時的無線網路拓撲架構圖通常會不一樣。為了要解決無線網

路節點的移動，我們利用時間戳記和路由路徑來建構出攻擊當時的無線網路拓撲架構圖，在 AP 端監控並修改整體時間戳記，使我們可以利用時間戳記建構出發生攻擊當時之網路拓撲圖，並且可以依此來追蹤攻擊者當時所在的位置。由於 AP 上採用利用 Pack logging 之 Hash based (bloom filter)，當攻擊者發動攻擊之後，由於其 Digest 儲存於路由器本身另外附加之記憶體，並會對應到路由器中的雜湊表格如圖 5。一旦受害者端遭受到攻擊時，受害者端會將其攻擊封包所對應之 Digest 送至該後端伺服器。當伺服器接收到該封包後，會查詢該 Digest 是否存在於該伺服器內，伺服器便可以基於 RGH 之路由資料，建構出攻擊者發動攻擊當時經過之感測器，並利用所經過之感測器建構出攻擊發動時該封包之攻擊路徑。

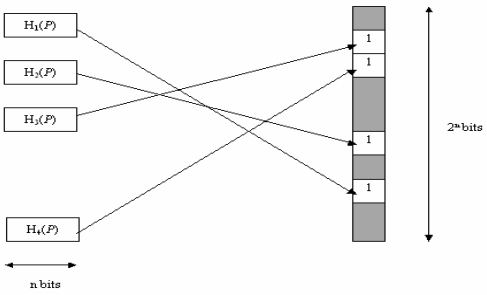

圖 5：Bloom Filter 儲存於路由器之 Digest

第三階段當收到多個攻擊追蹤警告後所啟動之移動攻擊拓撲圖合併階段以減少多餘之攻擊提示。當收到多個攻擊追蹤警告時，我們從 RGH 表將路徑以及時間戳記取出，還原當時網路拓撲的情形，接著檢查是否形成迴圈，如有迴圈則將之移除。再判斷攻擊者是否移動了位置，若兩次攻擊警告拓撲合併計算後發覺兩攻擊地點為攻擊者可能移動之範圍內，則將之視為同一攻擊者；由於該網路拓撲所有變化都因為時間戳記之不同而被標示，所以合併攻擊圖時可以依照時間戳記來判斷網路拓撲之變化，並判斷兩不同 IP 之攻擊者是否為同一人，以解決攻擊者假造多個 IP 企圖混淆追蹤的問題。

利用 nR24E1 實做感測器

首先我們將利用 nRF24E1 這包含了 8051CPU (最大 20MHz)與 Radio Transceiver 的硬體裝置來建置實驗環境。

我們選擇 nR24E1 來開發之原因主要有：

nRF24E1 對常用的 8051 晶片做了一些擴展，且 KeliC 51 V7.01 和他以上的版本都已經有支援 nRF24E1 了。nRF24E1 內含 8051 指令相容的 CPU 但是此 CPU 的 CPI(cycle per instruction)為工業標準 8051 的 0.33~0.41 倍,除了這裡有些許不同之外還包含了 PWM 和 SPI 端口 A/D 轉換器 nRF2401 無線收發 RTC 喚醒定時器 XTAL 和 RC 振蕩器等。耗電小且成本不高且內含了 Radio transceiver 可利用 nRF24E1 做許多無線系統相關的開發 例如無線電話、網路通訊等。

nRF24E1 特色是使用全球通用的 2.4GHz 頻率其速率為 1Mbps，只需一個晶振和一個電阻即可設計射頻電路，外圍元件極少，發射功率和工作頻率等所有工作參數全部可通過軟件設置，電源電壓範圍為 1.9-3.6v。工作功耗很低電流消耗很小。

nRF2401 的 ShockBurst™ RX/TX 模式採用片上先進先出(FIFO)來進行低數據率的時脈同步和高數據率的傳輸，因此極大的降低了功耗。ShockBurst™發射主要通過 MCU 接口引腳 CE、CLK1 和 DATA 來完成。設定 CE 為 high 此時會驅動版子上的 nrF2401 做資料處理，nRF2401 子系統檢查接收節點的位置(RX address)還有 payload data 完成後 CPU 會設定 CE 為 low，此時會驅動 ShockBurst™傳輸。

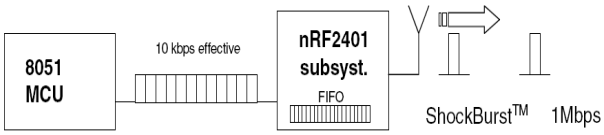

圖 6：ShockBurst™傳輸模式示意圖

然而 24E1 晶片中只有 4k 記憶體以及 CPU 效能限制，且其 code segment 只有 2K 位元組，因此目前無法實做全部之 DSR 協定於每個節點中，為了可以將封包透過感應器傳送，我們實做 DSR 中之 Route Discovery 以及 Route Maintenance 兩個功能。以維持最基本路由建立之功能來傳送封包至後端伺服器。

四.實驗結果

我們的實驗環境為空曠且節點間無任何障礙的教室，實驗空間約為十公尺見方，每個感測器之間距為約為 1~2 公尺，在這空間中共佈置使用 11 個 24E1 晶片和一台個人電腦(CPU Intel T2250,RAM 512MB,Wireless Card Intel 3945ABG)來模擬一個小型無線感測網路，利用小型感測網路來監聽附近之溝通封包以及用個人電腦來模擬 AP 接收所有感測器回傳之訊息，其中另外於網路中置入 1-3 個不等攻擊者，假設所有的攻擊者具有假冒 IP 和 MAC 位置之能力，且攻擊者具有可以攻陷合法節點來當成跳板進行攻擊的能力，所以在這環境中無法利用任何 IP 和 Mac 來辨識網路中之節點合法性，我們將這些節點佈置成如圖 7 之樹狀之網路拓撲。

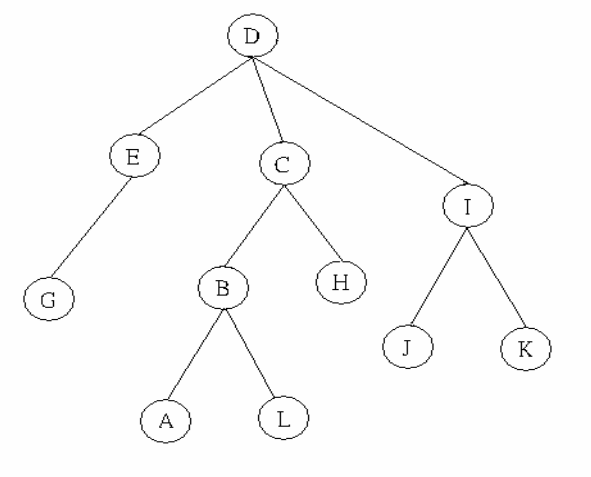

圖 7：節點位置示意圖

我們的實驗主要分成幾個類別，第一為將感測器以樹狀拓撲佈置於實驗環境中，只有一個移動的攻擊者，且這攻擊者不會改變 IP 的狀態下作分析與定位，結果如圖 8。第二為一個不會改變 IP 的攻擊者與整個無線傳輸環境都在作隨機移動的情況下，結果如圖 9。第三為一個會隨機變造 IP 的攻擊者但不移動位置與整個無線傳輸環境都不變動的情況下，結果如圖 10 和圖 11。第四為一個攻擊者移動且隨機變造 IP 與整個無線傳輸環境都在作隨機移動的情況下，結果如圖 12。第五為增加另一攻擊者攻擊者都在作隨機移動與整個無線傳輸環境都在作隨機移動的情況下，結果如圖 13。

我們實驗認定演算法成功找到攻擊者的條件為每一筆路徑新增至資料時，重建攻擊者路徑和數量的與實際的情形相同時視為成功，若是我們演算法將假裝網路中合法 IP 之攻擊者移動後和該合法攻擊者合併，以至於攻擊者數目減少則為失敗的合併攻擊者。另外，若是無法判斷一個移動且更換偽裝 IP 攻擊者為同一人，以致於攻擊者數目增加則我們認定我們的演算法失敗。以下所有實驗數據皆是同樣拓撲但所有節點之初始 IP 隨機產生 200 次實驗之平均值。

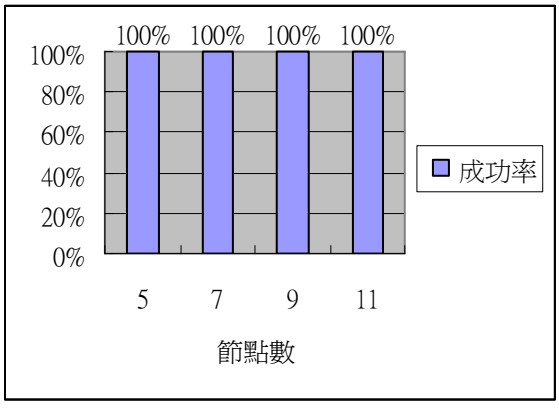

圖 8：攻擊者*1 攻擊者 IP 固定
攻擊者隨意移動 中繼節點不移動

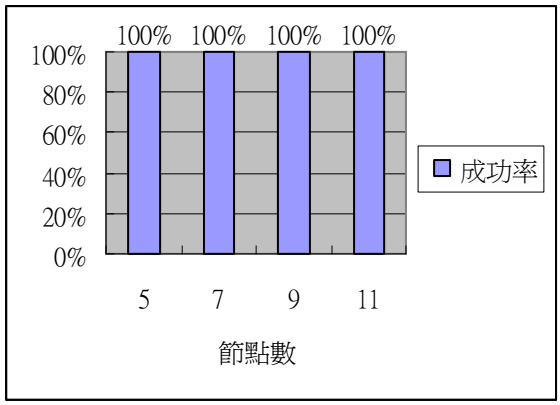

圖 9：攻擊者*1 攻擊者 IP 固定
攻擊者隨意移動 中繼節點隨意移動

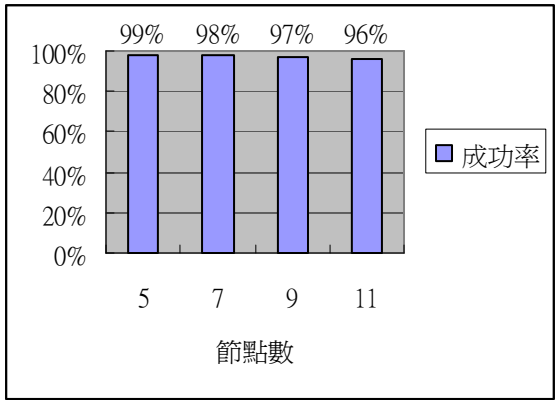

圖 10：攻擊者*1 攻擊者 IP 一直改變
攻擊者不移動 中繼節點不移動

由圖 10 發現當攻擊者隨意更換 IP 時，會開始產生誤判，發生誤判的次數與節點數成正相關。經由演算法所繪製出的攻擊拓撲得知，發生誤判的原因是一條路徑之中有相同的兩個(以上)IP。此時演算法會誤認為重複的 IP 發生 LOOP 而將其移除。為了降低誤判率，我們將同一條路徑上相同的 IP 先標誌起來並存入 Hash Table 後將之 IP 更換，之後需要時再去 Hash Table 查詢當時所使用之 IP。

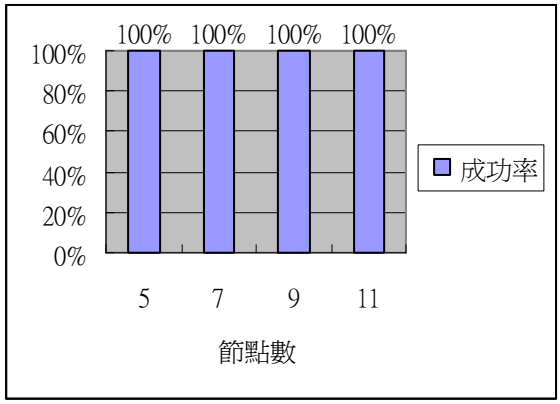

圖 11：攻擊者*1 攻擊者 IP 一直改變
攻擊者不移動 中繼節點不移動 改良後結果

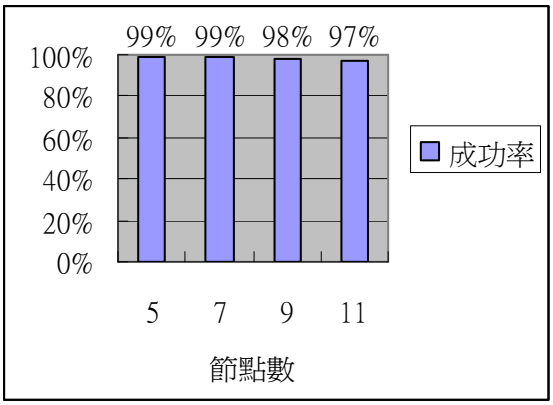

圖 12：攻擊者*1 攻擊者 IP 一直改變
攻擊者隨意移動 中繼節點隨意移動

由圖 12 發現當有一攻擊者在不斷更改 IP 且隨意移動時，誤判率開始增大，這是因為攻擊者移動的距離過大或是整個環境改變太大所造成，演算法會將其視為不同的攻擊者。

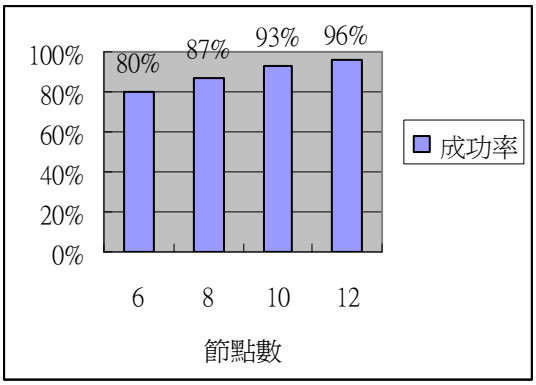

圖 13：攻擊者*2 攻擊者 IP 不改變
攻擊者隨意移動 中繼節點隨意移動

由圖 13 發現當節點越少時越容易發生誤判。其原因是節點數越少，兩攻擊者的攻擊行為越相近，因而造成演算法將兩攻擊者合併成同一個攻擊者。為了解決此問題，我們應當某一時間間隔內，行為相近的攻擊者大於某一數字再做合併。

五.結論

我們在本論文提出一個利用感測網路偵測無線網路攻擊封包，以追蹤無線移動匿名攻擊者之位置之方法，該方法改善 Hung 所提之 Hotspot traceback 因沒有分析不同時間傳送至該無線網路攻擊警告可能為同一攻擊者因移動而造成有多個警告的問題，我們增加追蹤的精準度和我們也可以合併因移動而造成之攻擊地點轉換之攻擊者。此外，我們將 WiTrack 被動的只有於 AP 蒐集各利用 DSR 繞境至 AP 之移動裝置來追蹤移動攻擊者，改為主動的利用於網路中佈置感測器來追蹤於無線網路中發動攻擊之移動匿名者以解決 WiTrack 只能追蹤攻擊者利用 DSR 送封包至 AP 而無法追蹤利用其他繞境方法之攻擊者。

另外，我們利用 nR24E1 晶片模擬真實無線網路環境中封包感測器，當攻擊發生時，我們能夠立刻利用感測器定位出其攻擊發起所在位置。就算攻擊者一直改變位置，我們也能夠及時隨著攻擊者改變攻擊路徑。即使攻擊者想使用變造 IP 的方式來混亂我們分析我們也幾乎可以分辨出其攻擊之來源是否為同一攻擊者。實驗結果中除了網路中同時存在 30%的偽造 IP 的攻擊者我們祇有 80 成功合併攻擊者外，其他的實驗我們都具有超過 97%可以成功分辨出攻擊者是否為移動後之同一匿名攻擊者而將兩個攻擊警訊合併。這結果將有利於我們中斷 DDoS 的攻擊，將被攻擊的損傷降到最低。

六.參考文獻

[1] 楊明豪,謝續平,“分散式癱瘓服務攻擊解決策略--追蹤匿名攻擊者,” 財團法人國家實驗研究院科技政策研究與資訊中心, 2006

[2] A. Belenky and N. Ansari, “IP Traceback with Deterministic Packet Marking,” IEEE Communications Letters, vol. 7, no. 2, pp. 162–164, Apr. 2003.

[3] Alex C. Snoeren, Craig Partridge, Luis A. Sanchez, Christine E. Jones, Fabrice Tchakountio, Stephen T. Kent, and W.Timothy Strayer, “Hash-Based IP Traceback,”in proceeding of the SIGCOMM’01, pp.27-31 August, 2001

[4] Burton H. Bloom, "Space/Time Trade-ORs in Hash Coding with Allowable Errors," Communication of ACM, vol. 13, no. 7, pp. 422-426, July 1970.

[5] David B. Johnson . David A. Maltz . Yih-Chun Hu ,”The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR),” draft-ietf-manet-dsr-10, July 2004

[6] Lawrence A. Gorden, Martin P Loeb, William Lucyshyn and Rober Richardson, “Computer Crime and Security Survey,” CSI/FBI, 2006

[7] M.-H. Yang, Warren Lin, C.-S. Chiu, and S.-P. Shieh, “Wireless Tracceback in Dynamic Source Routing,” TWISC 資通安全學術會議, 2007

[8] M. Adler, “Tradeoffs in Probabilistic Packet Marking for IP Traceback,” Proceedings of the thiry-fourth annual ACM symposium on Theory of computing, pp. 407–418, 2002.

[9] Nordic Semiconductor ASA, nRF24E1. Available: http://www.nordicsemi.no/

[10] S. Bellovin , M. Leech, and T. Taylor, “ICMP Traceback Messages,” Feb. 2003, available at: http://www.ietf.org/internet-drafts/draft-ietf-itrace-04.txt.

[11] S. M. Bellovin , “ ICMP trace back messages , ” Internet Draft: draft-bellovin-itrace-00.txt, 2000.

[12] SPIE,http://www.ir.bbn.com/projects/SPIE/

[13] Tao Peng, Christopher Lekie, and Kotagiri Ramamohanarao, “Ajusted Probabilistic Packet Marking for IP Traceback,” NETWORKING 2002, LNCS 2345, pp. 697-708, 2002

[14] Yi an Huang and Wenke Lee, "Hotspot-based traceback for mobile ad hoc networks," in WiSe '05: Proceedings of the 4th ACM workshop on Wireless security, New York, NY, USA, 2005, pp. 43-54, ACM Press.

[15] I. Cubic, D. Begušic, and T. Mandic, “Client based wireless LAN indoor positioning”, Telecommunications, 2005. ConTEL 2005. Proceedings of the 8th International Conference on, June 15-17, 2005, pp.335-339

[16] K. Kaemarungsi and P. Krishnamurthy, “Modeling of Indoor Positioning Systems Based on Location Fingerprinting”, School of Information Science, University of Pittsburgh, 2004

[17] Z. Xiang, S. Song, J. Chen, H. Wang, J. Huang, and X. Gao, “A wireless LAN- based indoor positioning technology” , IBM J. RES. & DEV., September/November 2004