行政院國家科學委員會專題研究計畫　成果報告

分散式阻斷服務攻擊來源快速追蹤 之研究與實作

計畫類別：個別型計畫
計畫編號：NSC94-2213-E-216-017-
執行期間：94 年 08 月 01 日至 95 年 07 月 31 日
執行單位：中華大學資訊工程學系

計畫主持人：王俊鑫

計畫參與人員：江彥志，夏怡華

報告類型：精簡報告
報告附件：出席國際會議研究心得報告及發表論文
處理方式：本計畫可公開查詢

中　華　民　國 95 年 10 月 30 日

行政院國家科學委員會補助專題研究計畫 □成果報告

分散式阻斷服務攻擊來源快速追蹤之研究與實作

計畫類別：□ 個別型計畫
計畫編號：NSC 94-2213-E-216-017
執行期間：94 年 8 月 1 日至 95 年 7 月 31 日

計畫主持人： 王俊鑫
計畫參與人員： 江彥志, 夏怡華

成果報告類型(依經費核定清單規定繳交)：□精簡報告

本成果報告包括以下應繳交之附件：
□出席國際學術會議心得報告及發表之論文各一份

處理方式：本計畫可立即公開查詢

執行單位：中華大學資訊工程學系

中 華 民 國 95 年 10 月 23 日

行政院國家科學委員會專題研究計畫成果報告

分散式阻斷服務攻擊來源快速追蹤之研究與實作

計畫編號：NSC 94-2213-E-216-017
執行期限：94 年 8 月 1 日至 95 年 7 月 31 日
主持人：王俊鑫助理教授　中華大學資訊工程學系
E-mail: chwang@chu.edu.tw

中文摘要

要探究攻擊來源，需藉由具有追蹤功能的路由器來幫忙，我們稱之為追蹤器(Tracer)。在本計劃中，我們探究該如何布建 Tracers 的位置及數量，才可有效的找到攻擊來源。在計劃中，我們探討如何以最少的 Tracers 的個數，來追蹤攻擊來源之布建問題，並證明此一問題為 NP-complete。因此，我們提出一個探索式 Tracers 的布建方法，可以保證任意攻擊來源與其攻擊封包經過的第一個 Tracer 的距離在可限定範圍之內。並且，我們可以事先計算出未偵測到攻擊機率的上限值(Upper Bound)，並將此值用來估算所設計布建方法中所須的 Tracers 數目。最後，藉由模擬程式的執行來量測 Tracers 布建問題之效能。為研究可過濾封包的路由器或交換器，為我們在個人電腦上，以多張網路卡實作一個具有防火牆、可過濾封包及可任意複製封包的交換器。

Abstract

To locate the attack origins, the traditional routers have to be enhanced with tracing service. The enhance routers are referred to as tracers. This project explores the tracers deployment problem for IP traceback methods how many and where the tracers should be deployed in the network to be effective for locating the attack origins. The minimizing the number of tracers deployment problems depended on locating the attack origins are defined. The problem is proved to be NP-complete. A heuristic method which can guarantee that the distance between any attack origin and its first met tracer should be within an assigned distance is proposed. The upper bound for the probability of an undetected attack node can be calculated in advance and used it to evaluate the number of tracers needed for the proposed heuristic method. Extended simulations are performed to study the performance of the tracer deployment. To study the filtering ability of a router or switch, we also implement a PC-based switch with functions of firewall, filtering and duplicating packets.

關鍵字：Tracer, IP Traceback

一、前言與研究目的

隨著網路技術的蓬勃發展，網路成為現今人們重要的溝通工具。但是隨伴而來的網路安全問題，確日益嚴重。從內部網路安全問題(Intranet security)，到網際網路安全問題(Internet security)；如阻斷服務攻擊(Denial of Service, DoS)、分散式阻斷服

務攻擊(Distributed of Service, DDoS)、蠕蟲式網路病毒的蔓延、電腦系統的漏洞等。在各種問題中，以佔用主機的資源或網路頻寬，導致主機無法對正常使用者提供服務的阻斷服務攻擊，最為嚴重與難解。因此，如何有效的解決阻斷服務攻擊及分散式阻斷攻擊的網路安全問題，實刻不容緩，為一重要研究課題。

分散式阻斷服務攻擊，事實上也是阻斷服務攻擊的另外一種型態，攻擊手法不再侷限以一個特定的通訊協定或特定系統弱點進行攻擊。其攻擊來源，通常源自多個被入侵的網路節點，幕後攻擊者可藉由簡單的指令，使得被佔領的網路節點，在同一時間內，分別以相同型態或不同的型態的阻斷服務攻擊，對相同一個伺服器發動攻擊，使得伺服器因大量的要求耗盡資源，造成癱瘓。

分散式的阻斷服務攻擊，因攻擊的來源不只一個網路節點，且攻擊的型態也不盡相同，所以如何有效解決分散式阻斷服務攻擊的問題，為一大挑戰。在文獻[1]中，探討如何防禦分散式阻斷服務攻擊，主要藉由一旦偵測到具有攻擊特徵的封包，則盡快過濾掉該類的封包，在文獻[2]中，更指出偵測節點的位置愈接近攻擊來源，可收集到的攻擊封包較少，愈不易偵測是否有攻擊的行為，因此增加偵測攻擊行為的難度，當偵測節點的位置但愈接近受害者，愈能有效的偵測是否有攻擊行為，如主機型與網路型的入侵偵測系統((Intrusion Detection System，IDS)，可以依據封包的特徵或數量，偵測到攻擊的事件，再藉由通知防火牆或封包過濾器進行過濾異常的攻擊封包，但往往過濾的節點的位置，離攻擊來源甚遠，防範的效果有限，因為從攻擊來源到過濾的節點之間的網路頻寬仍被佔用，而且無法得知攻擊的來源。

因此，如果可以掌握攻擊來源的路徑，就能在最接近攻擊來源做出適當措施，有效的過濾掉異常的攻擊封包，而且可以作攻擊事件的舉證，對攻擊來源進行追訴。有許多的文獻[3-15]，探討如何追蹤攻擊來源，稱為 IP 來源追蹤(IP Traceback)，因現行的網際網路通訊協定，路由器不會在 IP 封包上記錄其傳送的真實路徑，再加上封包的來源端 IP 位址很容易被偽造，攻擊者往往不是直接攻擊主機的，大多透過其它被入侵佔領的電腦，進行攻擊。對於受害者想要找出真正的攻擊者，實屬不易，但透過 IP 來源追蹤，不一定能找到真正幕後的攻擊者，但至少能找到幾近於攻擊來源，直接進行攻擊的主機。

在現行網路上，路由器只負責封包轉送的動作，為了支援追蹤來源 IP 的方法，必須增加路由器原有的功能，例如紀錄封包內容摘要(Digest)資訊，或者將路由器資訊寫入到封包內等功能。在本計劃中，具有支援追蹤來源 IP 功能的路由器，我們稱為追蹤器(Tracer)。文獻[16]中指出，在二千零三年五月初所收集到的路由器數目就高達十九萬兩千多，若將所有的路由器更新為 Tracers，所費不孜。因此有許多文獻中[3-7]，在部份布建 Tracers 的環境下，探討追蹤來源 IP 的方法，研究結果顯示，即使布建 Tracers 個數超過網路總節點一半時，仍然有漏網之魚，因為只要攻擊封包沒有經過任何 Tracers，再好的 IP Traceback 的技術亦無用武之地。事實上，Tracers 的位置將會影響追蹤攻擊來源的效能，因此，在本計劃中，我們將研究如何有效地布建 Tracers。

二、 文獻探討

在文獻[3-7]中所提出追蹤攻擊來源方法中，允許部份布建 Tracers，但都未深入探討到該如何有效部份布建 Tracers 的問題。若攻擊路徑部份的路由器未具有追蹤攻擊來源之功能，受害者端就無法收集到這些路由器之資訊，只能重建出部份的攻擊路徑，更嚴重的情況，當攻擊路徑上的路由器都不是 Tracers，攻擊來源將成為漏網之魚。而在文獻[8-10]中，將 Tracers 布建在邊緣路由器(Edge Router)或者邊界(Border Router)

路由器上，因為攻擊者傳送攻擊封包至網路時，須透過本地路由器轉送，似乎是不錯的 Tracer 布建方法，但如果攻擊封包來自於骨幹路由器所連接的電腦，將導致無法有效追蹤到攻擊來源。

Savage 等人[3]提出封包標記機率方法中，路由器具有標記封包的能力，作為追蹤攻擊來源目的。當封包經過路由器，封包被路由器標記時，路由器會將本身訊息寫到封包 IPv4 標頭(header)內的 Identification 欄位中。因標頭內的 Identification 欄位僅僅只有 16 位元，作者利用分段(fragmentation)與 XOR(exclusive-or)的技術將路由器的位址壓縮並切割成 16 位元。受害者收集足夠封包後，藉由統計分類動作，即可找出攻擊來源。具有標記能力的路由器，可以採取逐步布建(incrementally deployed)方式，但作者未針對布建方式進一步的深入探討。

Song 等人[4]提出方法中，當封包被路由器標記到時，將路由器本身位址產生 8 位元雜湊數值(hash)後，路由器會將雜湊數值寫到封包 IPv4 標頭內的 Identification 欄位中。受害者欲重建攻擊路徑，前提必須有網路拓樸結構圖。受害者收集足夠封包後，藉由統計分類動作，來找出攻擊來源。具有標記能力的路由器，可採取逐步布建方式，但作者仍未針布建方式的影響作進一步的探討。

由 Choi 等人[5]提出方法中，路由器會針對每個介面(interface)流量作統計，依據介面資料的多寡，進行霍夫曼編碼(Huffman code)，流量較多的介面會有較短的霍夫曼編碼，路由器動態的維護每一個介面的編碼結果，並將介面的編碼寫入流經的封包內，當受害者欲重建攻擊路徑，只要將收到封包內編碼的串列，向上游的路由器中進行查詢動作，則可知封包是由路由器的哪個介面進入，再繼續往上游路由器進行查詢，直到串列處理完畢，就可以重建出攻擊來源路徑。作者並提到，封包傳送過程中，若有些路由器未將標記資料寫入到封包中，會導致解碼錯誤，無法重建出攻擊路徑。

由 Bellovin 等人[6]提出方法中，有支援 ICMP 的路由器又稱 i-Trace Router。i-Trace Router 以 1/20,000 的機率標記經過的封包，路由器會依據封包目的位址，再傳送一個 ICMP 封包到目的端，ICMP 封包紀錄內容為路由器本身的資訊；當受害者收集到足夠的 ICMP 封包後，藉由統計動作，即可重建出攻擊來源路徑，但未探討對如何布建 i-Trace routers。

由 Soneren[7]提出方法，只需要一個封包就即可重建出攻擊路徑。這個方法是以 SPIE(Source Path Isolation Engine)架構為基礎。SPIE 系統由 Data Generate Agents (DGAs)、SPIE Collection and Reduction Agents(SCARs)和 SPIE Traceback Manager(STM)所組合而成。DGAs 是指路由器具有擷取封包資訊並產生雜湊數值後，將雜湊值儲存在路由器空間內，路由器藉由儲存的雜湊值可以判斷封包是否由自己轉發出去。SCARs 負責管理 DGAs，並能重建封包在所管理的 DGAs 內所傳送的路徑。STM 能控制所有的 SPIE 系統，並能重建攻擊路徑。當受害者欲追蹤攻擊來源，將攻擊封包特徵傳至 SPIE 系統內的 STM，STM 會把封包特徵傳送給每個 SCARs，SCARs 將封包特徵傳送給 DGAs，由 DGAs 進行比對查詢動作，並將比對結果回傳至 SCARs，SCARs 收到 DGAs 結果後，進行重建部份攻擊路徑，並將路徑回傳給 STM，STM 再根據收到 SCARs 的部份路徑進行重建後，就是整個完整的攻擊路徑，再回傳給受害者。作者所提出的方法是可以支援逐步布建 SPIE 系統，並且不需每個路由器具有 DGAs(也就是我們所稱的 Tracers)的功能。DGAs 布建的位置也可以部份佈建，或者是布建在邊緣路由器上，但未探討如何有效的布建系統中的 DGAs 及

SCRs。

當攻擊封包未經過任何的 Tracers，再好的 IP Traceback 的技術亦無用武之地，換句話說，將無法追蹤到攻擊來源。事實上，Tracers 的位置跟數目將會影響追蹤攻擊來源的效能。布建 Tracers 位置不佳的話，使得攻擊封包經過 Tracers 的機會減少，因此無法有效追蹤到攻擊來源。布建 Tracers 數目太少，也會使得封包經過 Tracers 機會減少，因此無法有效追蹤到攻擊來源。

三、研究方法與模擬結果

在成本的考量下，僅有部份的路由器更新為 Tracers，要如何有效的布建 Tracers？由於攻擊者位置很難預料，若攻擊封包沒有經過任何的 Tracers，則無法追蹤到攻擊來源，因此，我們想要解決的**第一個布建 Tracers 問題為：如何布建最少的 Tracers 數目，可以保證任一攻擊路徑中，至少會經過一個 Tracer。**

在採取部份布建 Tracers 的網路環境下，想要找出準確的攻擊來源，似乎有點難度，若能找到攻擊封包經過的第一個 Tracer，再藉由它進一步找出攻擊來源的位置，較為可行。此外若 Tracers 具有過濾(Filter)封包功能的話，則在攻擊封包經過的第一個 Tracer 時，就可以把攻擊封包過濾掉，可避免攻擊封包繼續傳送到受害者端的過程所造成的頻寬浪費。因此，找出攻擊來源位置所需的成本和保護頻寬多寡與攻擊來源至其攻擊路徑上的第一個 Tracer 之距離有關。因此，我們想藉由 Tracers 布建的方法來控制此距離，讓此距離在可限定的範圍之內。所以**第二個想要解決的問題為：要如何布建最少的 Tracers 數目，可以保證任意攻擊來源至其攻擊路徑上第一個 Tracer 的距離在 s hop count 之內。**

仔細的推敲，事實上，上述的第一個問題為第二個問題的子問題，因此只要解決第二個問題，就可以解決我們所提出的 Tracers 布建的問題。而為了解決 Tracers 布建的問題，我們將此問題對應為圖論問題，並定義為 K-diameter-cut 問題，且證明 K-diameter-cut 問題是一個 NP-complete，證明的過程可參考我們發表的計劃研究成果[17]。因為 K-diameter-cut 問題是一個 NP-complete，所以我們提出一個探索(heuristic)方式來解決布建 Tracers 問題，稱之為 K-diameter-cut 演算法。

K-diameter-cut 演算法主要構想為從圖形 G 的中心集合挑選任一頂點為起始點，找到第一個子圖直徑小於 K(K>1)；而第一個子圖相鄰的頂點就是我們想要佈建 Tracers 的頂點，接著我們將第一個子圖及其相鄰頂點從原本圖形 G 中刪除，則原本圖形 G 會變成數個連通的子圖；若子圖其直徑大於等於 K，則再依此遞迴(recursive)。K-diameter-cut 演算法如下：

K-Diameter-cut 演算法

輸入：一個圖形 $G = (V, E)$

輸出：合適的 *K-Diameter* cut T

1）若 $K = 1$，則先呼叫 Erd¨os Greedy[18]演算法，求得頂點的獨立集合 S;然後

$V-S$，即為解答。否則執行下面步驟。

2）計算每個頂點$e(v)$值，$v \in V$。(在圖形 G 中，頂點v的離心率(eccentricity)記為$e(v)$，是代表以頂點 v 與頂點 u 最長的距離，換言之就是$e(v) = max\{ d(u,v), where \ u \in V \}$)。

3）從圖形 G 中，找出由最小值的$e(v)$的頂點所構成的中心點集合，從中心點集合中，挑選任一頂點 c。

4）當 K 為奇數時，拜訪與 c 頂點距離為$(k-1)/2$ 的所有頂點。令這些頂點的集合為 W，$W = \{ v | \ d(v, c) \leq (k-1)/2 \text{ and } v \in V \}$。

5）當 K 為偶數時，則執行下列子步驟。

a）拜訪與 c 頂點相鄰距離為$\lfloor (k-1)/2 \rfloor$的所有頂點。這些頂點的集合為 W，$W = \{ v | \ d(v, c) \leq \lfloor (k-1)/2 \rfloor \text{ and } v \in V \}$。

b）找出 $Y = \{ v | \ d(v, c) = \lfloor (k-1)/2 \rfloor + 1 \text{ and } v \in V \}$。

c）任意選擇頂點$v_y \in Y$，並將v_y從 Y移除掉。

d）若 $d(G_{W \cup \{v_y\}}) < K$，將$v_y$加入到 W(換言之 $W = W \cup \{v_y\}$)。

e）若 $Y \neq \phi$，則重複子步驟(c)和(d)。

6）在 G 中，將子圖G_W收縮後變成一個頂點v_w，獲得圖G^*。

7）將v_w的相鄰頂點放入 T 中(T初始值 = 0)；並將v_w及其v_w相鄰的頂點從G^*移除，獲得圖G'。

8）在G'中每個子圖G_i，若 $d(G_i) \geq k$，則一直遞迴G_i，並重複執行 2～8 的步驟。

模擬結果

我們將採用 BRITE[19][20]工具軟體產生網路拓樸結構圖，每個網路節點代表是一個路由器，每個邊的成本都是 1 hop 距離，封包以最短路徑來傳送;在我們的模擬實驗不考量傳送路徑改變的影響。

在圖一中，模擬實驗中利用 BRITE 分別隨機產生 degree = 4 和 6(d = 4 和 d = 6)各 25 張網路拓樸結構圖，每張圖均 1000 個網路節點;用我們提出的 K-diameter-cut 方法，計算出每個 K-diameter area 平均涵蓋多少個網路節點(如圖一左邊 y 軸虛線所示)及計算出平均 K-diameter area 數目(如圖一右邊 y 軸所示實線所示)。從圖中，我們可以明顯的發現當 d = 6 時，K-diameter area 平均涵蓋網路節點數目在大當 d = 4 的環境，這是因為 degree 愈大，網路節點連接較多的網路節點，就有愈多的網路節點被包含進 K-diameter area。相對的，平均 K-diameter area 數目在 d= 4 時反而大於當 d= 6 的環境，因為 degree 愈大，每個 K-diameter area 可包含更多的網路節點，則 K-diameter area 數目就會愈少。

圖二與圖三分別為當 d = 4 和 d = 6 布建 Tracer 的密度(ρ = Tracers 個數/所有的網路節點個數)；由 BRITE 軟體工具產生 d = 4 和 d = 6，各 50 張不同的網路拓樸結構圖，每張圖的網路節點個數為 N從 100 到 1200。從圖二與圖三中可以清楚發現，當 K = 1 時，無論網路節點個數為多少，值 ρ 幾乎趨進於固定的值，這個資訊可以評估需要布建多少 Tracers 數目才可以保證，不管攻擊者在網路的任何地方，任何的攻擊路徑中至少會經過一個 Tracer。另外，值的一提的是愈高的 K 值，則 ρ 值會減少；那是因為在我們提出的 K-diameter-cut 方法，若 K 值愈大，則每次會有更多的網路節點被包含到 K-diameter area，故所需的 Tracers 就會變少。從圖中也可以明顯發現，在 K-diameter-cut 方法內，若中心點集合中，包含一個以上的網路節點，選擇 degree 比較大的網路節點為中心點的方式比任意挑選一點為中心點的方式得到值 ρ 還低。這是可以解釋的，選擇比較大的 degree 網路節點當為中心點與其相鄰的網路節點就愈多，就會有愈多的網路節點被包含到 K-diameter area 內，所以 Tracers 就變少。

接著，我們針對 K-diameter-cut 布建 Tracers 的方法，探討未偵測到攻擊來源機率的多寡。K-diameter-cut 方法能提供布建多少個 Tracers，保證攻擊者在 s hop 距離內，一定遇到 Tracers，若攻擊者在和受害者距離小於 s hop 距離內，則就無法偵測到攻擊來源。從網路的拓樸結構，可以計算出任意兩個網路節點的距離，所以任意兩個網路節點距離為 h hop 的機率亦可算出，當 $\varphi(h)$已知，可以估計當攻擊者和受害者的路徑距離小於 s hop 距離內，它們的機率是多少，做為未偵測到攻擊者上限的機率，其計算方式如下：

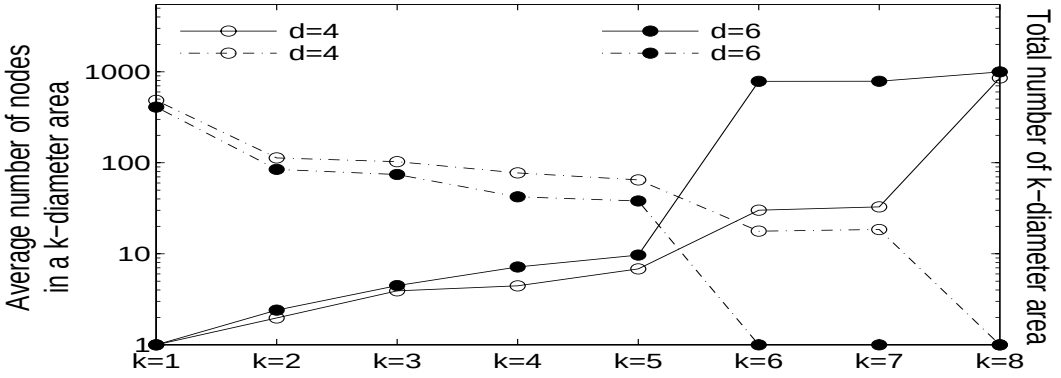
$$P_{ub} = \sum_{1}^{s-1} \phi(h)$$

圖四是代表未偵測到攻擊者上限的機率(P_{ub})和模擬發生攻擊狀況後的結果。由 BRITE 隨機產生 25 張圖，分別為 d = 4 跟 d = 6，每張圖為網路節點 1000 個，在每張圖上，模擬 DDoS 攻擊，隨機產生 50 個攻擊者和一個受害者。在圖四中，虛線顯示未偵測到攻擊者上限的機率 P_{ub} 值，實線顯示以 K-diameter-cut 布建 Tracers，模擬 DDoS 攻擊，統計未偵測到攻擊者機率之結果。在圖四中，我們明顯的發現，在不同 K 值狀況下，P_{ub} 值都大於實際未偵測到攻擊者的機率。由 P_{ub} 值的大小，可以幫助我們挑選合適的 K 值，作為執行 k-diameter-cut 演算法的依據，例如 K = 5，d = 4 的 P_{ub} 值是 0.31769，然而當 K = 5 ，d = 6 的 P_{ub} 值太大了。

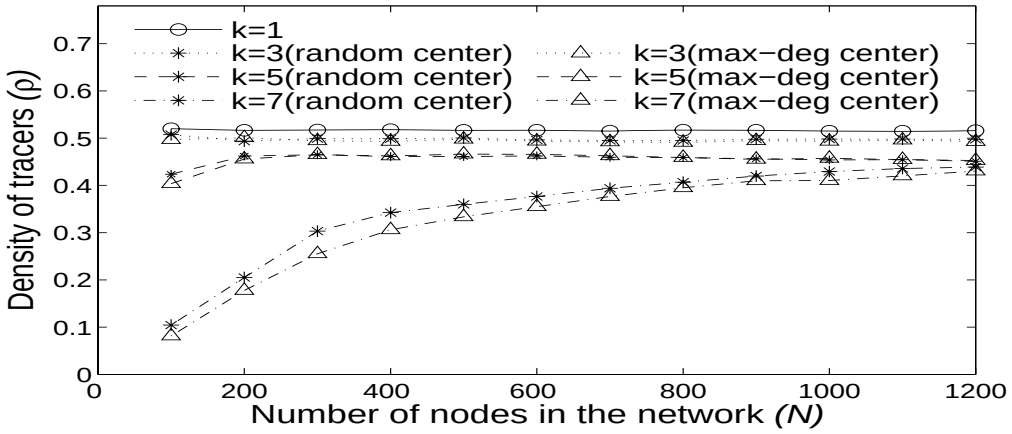
四、計畫自評

如何追蹤出攻擊來源，在 IP traceback 方面的相關文獻大多著重於如何找出攻擊者的方法，對於布建 Tracers 的方法，並沒有太多著墨。本計劃中，我們研究如何在網路上有效的布建 Tracers；定義布建 Tracers 的問題，並提出 K-diameter-cut 演算法提供有效的布建 Tracers，使得在網路上任何地方的攻擊者，其攻擊封包在 s hop 距離內一定會遇到一個

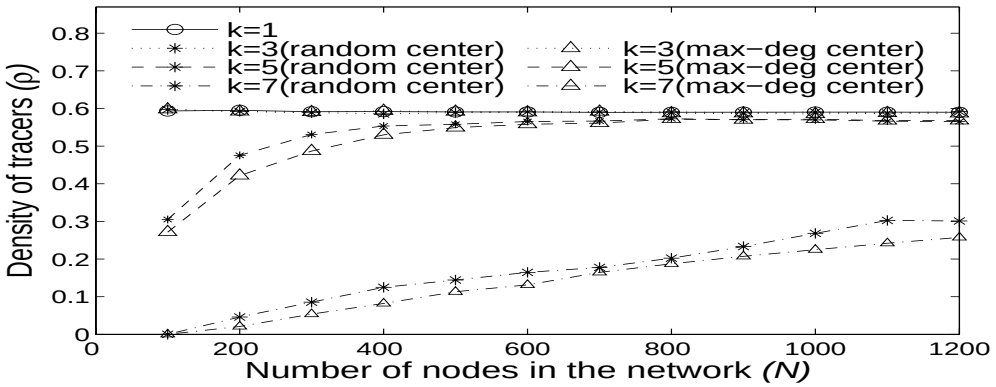
Tracer。而且藉由網路的拓樸結構，可以估算未偵測到攻擊者機率的上限值，並藉由此值評估 *K*-diameter-cut 演算法中合適的 *K* 值，以估算所須的 Tracers 數目。相關的研究成果，論文發表在 2006 ACM/IWCMC[17]的會議。再者為了要實作一個可過濾封包的路由器或交換器，我們在個人電腦上，以多張網路卡實作一個具有防火牆、可過濾封包及可任意複製封包的交換器，相關的研究成果既將發表在 2006 TANET 的會議[21]。而參與本計畫之研究人員，藉由規劃目標、執行過程、結果分析、延伸應用，培養出網路安全與具備實作能力的科技人才，以落實前瞻產業技術建立及人才培育的目標。



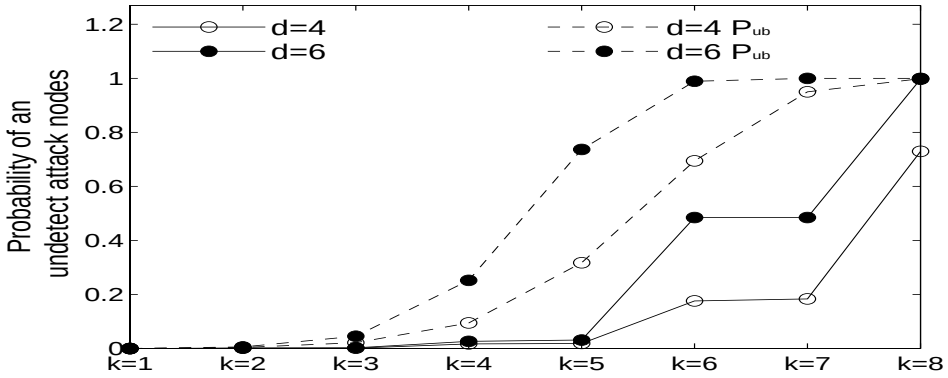
圖一：*K*-diameter area 個數及涵蓋範圍



圖二：*d* = 4 Tracers 的布建密度



圖三：*d* = 6 Tracers 的布建密度



圖四：未偵測到攻擊者的機率

參考文獻

.

[1] J. Lee and G. d. Veciana, "Scalable multicast based filtering and tracing framework for defeating distributed DoS attacks," *International Journal of Network Management*, 2005, pp. 43-60

[2] D. Basheer, A. Chakrabarti, and G. Manimaran, "Efficient dynamic probabilistic packet marking for IP traceback," *Proc. 3rd IFIP-TC6 Networking*, May 2004, pp. 1263-69.

[3] S. Savage, D. Wetherall, A. Karlin, and T. Anderson, "Network Support for IP Traceback," *In ACM/IEEE Transactions on Networking* vol. 9, no. 3, June 2001, pp. 226-37.

[4] D. X. Song and A. Perrig, "Advanced and Authenticated Marking Schemes for IP Traceback," *Proceedings of the IEEE INFOCOM*, 2001, pp. 878-86.

[5] K. Choi and H. Dai, "A Marking Scheme using Huffman Codes for IP. Traceback," *Proc. ISPAN*, 2004, pp. 421-28.

[6] S. M. Bellovin, "ICMP Traceback Messages," IETF draft, 2000; htttp://www.research.att.com/smb/papers/draftbellovin-itrace-00.txt.

[7] A. C. Soneren et al., "Single-packet IP Traceback," *IEEE/ACM Transactions on Networking*, vol. 10, Dec. 2002, pp. 721-34.

[8] T. Baba and S. Matsuda, "Tracing Network Attacks to Their Sources," *IEEE Internet Computing*, vol. 6, no. 3, 2002, pp. 20–26.

[9] A. Belenky and N. Ansari, "IP Traceback with Deterministic Packet Marking," *IEEE Communications Letters*, vol. 7(2), Apr. 2003, pp. 162-64.

[10] R. Stone, "CenterTrack An IP overlay network for tracking DoS floods," in *Proc. 2000 USENIX Security Syrup*, July 2000, pp. 199-212.

[11] H. Y. Chang *et al.*, "Deciduous: Decentralized Source Identification for Network-Based Intrusions," *Proc. 6th IFIP/IEEE Int'l. Symp. Integrated Net. Mgmt.*, 1999.

[12] H. Burch and B. Cheswick, "Tracing Anonymous Packets to Their Approximate Source," *Proc. USENIX LISA*, 2000, pp. 319–27.

[13] A. Yaar, A. Perrig, and D. Song, "FIT: Fast Internet Traceback," *Proc. INFOCOM*, 2005, pp. 1395-1406.

[14] U. K. Tupakula, and V. Varadharajan, "A proactical method to counteract denial of service attacks," *in Proc. Australasian Computer Science Conference* (ACSC2003), Adeliaide, australia. Conference in Research and Practice in Information Technology, vol. 16.

[15] T. Doeppner, P. Klein, and A. Koyfman. "Using Router Stamping to Identify the Source of IP Packets," In *7th ACM Conference on Computer and Communications Security*, November, 2000, pp. 184-189.

[16] http://www.caida.org/tools/measurement/skitter/router_topology/

[17] C.-H. Wang, C. W. Yu, C.-K. Liang, K.-M. Yu, W. Ouyang, C.-H. Hsu, and Y.-G. Chen,

"Tracers Placement for IP Traceback against DDoS Attacks," *International Wireless Communications and Mobile Computing Conference*, Vancouver, Canada, pp. 355-360, 2006. (included in **ACM Digital Library**)

[18] P. Erdös, "On the graph-theorem of Turán," Math. Lapok, vol. 21, pp. 249-251, 1970.

[19] A. Medina, A. Lakhina, I. Matta, and J. Byers, BRITE: An Approach to Universal Topology Generation, In Proceedings of the International Workshop on Modeling, Analysis and Simulation of Computer and Telecommunications Systems-MASCOTS '01, Cincinnati, Ohio, August 2001.

[20] O. Heckmann, M. Piringer, J. Schmitt and R. Steinmetz, "Generating Realistic ISP-Level Network Topologies," *IEEE Communications Letters*, 7(7):335–337, July 2003.

[21] 楊有信，王俊鑫 "可動態洞悉、管理內部網路安全之研究與實作," TANET 2006.