行政院國家科學委員會專題研究計畫 成果報告

可防禦分散式 DDoS 攻擊的異質性追蹤器布建問題之研究(II)
研究成果報告(精簡版)

計 畫 類 別 ：個別型
計 畫 編 號 ：NSC 99-2221-E-216-017-
執 行 期 間 ：99 年 08 月 01 日至 100 年 10 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
共 同 主 持 人：翁文彥
計畫參與人員：碩士級-專任助理人員：蕭裕鴻
碩士級-專任助理人員：朱健豪

報 告 附 件 ：出席國際會議研究心得報告及發表論文

公 開 資 訊 ：本計畫涉及專利或其他智慧財產權，2 年後可公開查詢

中 華 民 國 101 年 01 月 13 日

中 文 摘 要 ： 要有效解決 DoS/DDoS 的問題，首先需找到攻擊來源，並協同鄰近的具有封包過濾功能
的路由器，即時的過濾異常封包，才能避免攻擊來源與受害者之間的網路頻寬被佔用。但
原有的路由器，並不具備追蹤、過濾封包等功能，我們必須在路由器增加新的功能來支援，
新增功能的路由器，我們以追蹤器來統稱。然而攻擊來源追蹤的效能，則與追蹤器的數量
及布建的位置息息相關。
在我們先前研究中，追蹤器環繞方式布建在網路區域的周圍，我們稱此區域為保護區
域，布建的方式可保證攻擊路徑在限定的長度之內，至少經過一個我們所布建的追蹤器，
且攻擊來源可追朔源自於那一個保護區域內，但當保護區域內節點數量過多的時候，就須
花費較多成本來搜尋攻擊者來源。 在計畫中，我們提出五種方法來改善先前文獻的問題，
可依成本的多寡，來控制劃分保護區域範圍內節點的數量，以控管攻擊者來源的搜尋成本。
藉由模擬結果，我們提出的布建方法，僅需增加額外少量的追蹤器成本，可有效的限制保護區
域內節點數量。

中文關鍵詞： 分散式阻斷服務攻擊、追蹤器

英 文 摘 要 ： To solve the DoS/DDoS problems efficiently, the first things is to locate the attack origins and then cooperate the filtering-enabled routers nearby to filter the abnormal packets in time. But the original routers can’t provide these functions such as tracking, filtering, and etc. They have to be enhanced with additional functions to defense DoS/DDoS attacks. We refer the enhanced routers to as tracers. But the performance of locating attack origins will depend on the number of deployed tracers and location of them.
In our previous work, tracers are placed to surround a network area which we referred to as protection area. Attack path can be guaranteed to travel at least one tracer within a limit hop count and attack origins can be traced back to which protection area is. But the cost of searching attack origins will be

high once the number of nodes in protection area is too many. In this project, we proposed five methods to improve previous work by bounding the number of nodes in each protection area. Simulation results show that our proposed methods can limit the number of nodes in protection areas with little extra tracers compared to previous work.

英文關鍵詞： Tracers, DDoS

行政院國家科學委員會專題研究計畫成果報告

可防禦分散式DDoS 攻擊的異質性追蹤器布建問題之研究（II）

計畫編號：NSC 99-2221-E-216 -017 -
執行期限：99 年 8 月 1 日至 99 年 10 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

要有效解決DoS/DDoS的問題，首先需找到攻擊來源，並協同鄰近的具有封包過濾功能的路由器，即時的過濾異常封包，才能避免攻擊來源與受害者之間的網路頻寬被佔用。但原有的路由器，並不具備追蹤、過濾封包等功能，我們必須在路由器增加新的功能來支援，新增功能的路由器，我們以追蹤器來統稱。然而攻擊來源追蹤的效能，則與追蹤器的數量及布建的位置息息相關。

在我們先前研究中，追蹤器環繞方式布建在網路區域的周圍，我們稱此區域為保護區域，布建的方式可保證攻擊路徑在限定的長度之內，至少經過一個我們所布建的追蹤器，且攻擊來源可追朔源自於那一個保護區域內，但當保護區域內節點數量過多的時候，就須花費較多成本來搜尋攻擊者來源。 在計畫中，我們提出五種方法來改善先前文獻的問題，可依成本的多寡，來控制劃分保護區域範圍內節點的數量，以控管攻擊者來源的搜尋成本。藉由模擬結果，我們提出的布建方法，僅需增加額外少量的追蹤器成本，可有效的限制保護區域內節點數量。

英文摘要

To solve the DoS/DDoS problems efficiently, the first things is to locate the attack origins and then cooperate the filtering-enabled routers nearby to filter the abnormal packets in time. But the original routers can’t provide these functions such as tracking, filtering, and etc. They have to be enhanced with additional functions to defense DoS/DDoS attacks. We refer the enhanced routers to as tracers. But the performance of locating attack origins will depend on the number of deployed tracers and location of them.

In our previous work, tracers are placed to surround a network area which we referred to as protection area. Attack path can be guaranteed to travel at least one tracer within a limit hop count and attack origins can be traced back to which protection area is. But the cost of searching attack origins will be high once the number of nodes in protection area is too many. In this project, we proposed five methods to improve previous work by bounding the number of nodes in each protection area. Simulation results show that our proposed methods can limit the number of nodes in protection areas with little extra tracers compared to previous work.

關鍵字：分散式阻斷服務攻擊、追蹤器； Tracers, DDoS

一、前言與研究目的

網路技術的蓬勃發展與日廣泛的應用，使得大量的資訊傳遞、交流，盡在彈指之間，網路已成為現今與未來人類不可或缺的工具。但伴隨而至的網路安全問題卻持續發燒，如蠕蟲式(worm)網路病毒的蔓延、以佔用主機資源或網路頻寬，導致主機無法對外提供服務的阻斷式攻擊(Denial of Service; DoS)、分散式阻斷服務攻擊(Distributed DoS; DDoS)[1,2] 及日新月異的入侵方式等，層出不窮的網路安全問題，長久以來，似乎是沒有百分之百的解決方法，如何有效的解決這些網路安全的問題，成為重要的研究課題。

DDoS 攻擊的特性，在於產生大量的攻擊封包肆虐網路頻寬，受害的主機因處理攻擊封包而耗盡過多的資源，導致無法對外提供正常服務。若能找到攻擊來源並即時過濾惡意封包，就能有效的解決 DDoS 的問題，因此攻擊來源的追蹤為解決 DDoS 問題的主要關鍵。

有許多的文獻[3-18]，探討如何追蹤攻擊來源，稱為 IP 來源追蹤(IP Traceback)；透過 IP 來源追蹤，雖然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，甚至直接進行攻擊的主機。IP 來源追蹤的方法，均需要在路由器增加新的功能來支援，在本計畫中，我們將升級後的路由器我們稱為異質性的追蹤器，以追蹤器(tracers)來統稱之。

事實上，以成本的考量，無法在短期內，將網路的路由器均升級為追蹤器，所以僅有部份的追蹤器存在，但追蹤攻擊來源的效能，實與追蹤器的布建及其數量息息相關。但目前有關 IP 來源追蹤的方法中，未對追蹤器的布建作深入的探討，大部份為任意布建的方式(random deployment)，少數以 ISP(Internet Service Provider)的邊界路由器(edge/boundary routers)，為追蹤器選擇的對像，雖然較易追蹤攻擊來源來自於那一個邊界路由器，但當攻擊來源發自於 ISP 內部的網路，就會面臨無法追蹤的窘態。在 97 年度的計畫中，以 marking-enabled tracers、filtering-enabled tracers 與 tunneling-enabled tracers 三種異質性的追蹤器，來探討如何有效的防禦 DDoS 的攻擊。在該計畫中，我們在各種追蹤器為隨意布建的環境下，研究如何有效的利用 tunneling-enabled tracers 適時的將封包導向最佳的 marking-enabled tracers 或 filtering-enabled tracers 以進行來源追蹤及即時過濾異常封包，但對於異質性的追蹤器的布建問題，仍有待深入的討論。

有關追蹤器的布建問題，我們有部分的研究成果[19,20]，可以保證封包的傳送路徑在一定的距離 k, 一定會經過我們所布建的追蹤器，但 k 與追蹤器的數量互為消長，k 過大時，當攻擊封包的路徑小於 k，亦無從追蹤，而且追蹤器的性質、功能，所須的成本多寡，升級的難易度等因素，會影響其在實際網路中佔有的個數比例，因此，本計畫我們延續先前的計畫，依追蹤器數量的多寡等，深入的研究異質性的追蹤器的布建問題，對攻擊來源追蹤的影響與過濾異常封包的效能的影響。

二、文獻探討

目前有關 IP 來源追蹤的研究，大致可區分為四類：(1)IP Marking [3-9] (2)ICMP Traceback [10-13] (3)Logging-based[14-17] (4)Overlay Networks [18]，著重於追蹤方法的設計，而有關於追蹤器的布建問題則較少如[19-23]，資將有關追蹤器布建的文獻敘述如下:

Seok Bong Jeong 等人提出 “An Effective Placement of Detection Systems for Distributed Attack Detection in Large Scale Networks”[21]，方法為以節點連接度(degree)最少的節點當起始點，考慮離起始點(R-1)個 hop count 範圍之外的周圍節點，作為布建追蹤器的位置，如此重複相同的步驟，直到整個網路節點都被涵蓋，但其演算法以選定的起始點來計算路徑，在選擇(R-1)範圍內的節點，會漏掉一些節點，因此 Islam, M.H 等人提出“Optimal Placement of Detection Nodes against Distributed Denial of Service Attack”[22]，來改善此方法的缺點，使得在整個網路節點挑選佈建追蹤器時相較於[21]更少。

在文獻[23]中，探討過濾器布建最佳化的問題，文中的過濾器無法識別封包的好壞，只能將通往受害端的封包一律過濾，布建的位置也僅限於 ISP 的邊界路由器(edge

routers)，以通往受害端的封包中，正常封包與攻擊封包的比例，利用動態程式規劃來分析，找出那些邊界路由器需設置過濾器，才會使得受害端在有限的頻寬下，可接受最多正常封包的流量為目標作最佳化，但要得知正常封包與攻擊封包的比例，往往要經過一段時間的量測與統計，再加上動態程式規劃所需的時間，才能決定過濾器最佳的布建位置，對防禦 DDoS 的攻擊，可能緩不濟急，而且當攻擊來源發自於 ISP 內部的網路，就會面臨無法追蹤的窘態。

我們之前的研究，K-diameter cut 方法[19]的演算法，雖然可以確保在一定的距離 *k*, 一定會經過我們所布建的追蹤器，但所找出來的保護區域內的節點數量無法控制，在確定攻擊來源落在某個保護區域內後，若其涵蓋的數量過多，恐影響搜尋攻擊來源的時間，因此之後，我們又提出了階層式 K-diameter cut 的演算法[20]，階層式 K-diameter cut 的方法為透過遞迴的方式，在過大數量的保護區域內，重複執行 K-diameter cut 演算法，以降低保護區域內節點的數量，降低搜尋攻擊來源的成本，但每一個保護區內節點個數的分布，還是可能出現多寡不均情況，且追蹤器的數量也因此增加，因此，在本計畫中，我們想要只找出可以控制保護區內節點的數量，且盡量讓每一保護區內節點的數量大致一樣，以有效的估算布建成本，及增加搜尋攻擊來源的效率。

三、研究方法與模擬結果

(a)研究方法

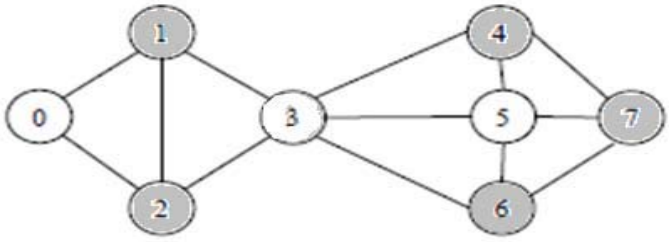
在本計畫，我們提出可限制保護區域節點數量演算法，以下為演算法所用的符號，定義如下：

- 由追蹤器所保護的區域，稱為保護區域 PA(Protection Area)。
- 保護區域範圍內，任兩點的距離小於長度 R 的路徑(hop counts)。
- 保護區域內節點數量的臨界值為 B。
- 為減少所需追蹤器的數量，在選擇追蹤器的位置進行調整，允許保護區域內節點少量的增加，增加的數量為 F，F 的預設值為⌈B*0.1⌉。

在限制 PA 內節點的數量的原則下，提出五種演算法如下:

●最大連接度節點優先挑選的布建方法**(LN_MAXDP)**

- 演算法目的在於盡可能選取較多的節點，在同一保護區域內。以連接度數量最多的點做開始來挑選，能挑到的鄰居點數會較多，因此保護區域內節點可涵蓋的點數可能較多，期望劃分出保護區域數較少，讓所需追蹤器數量較少，但相對的周圍的節點亦多，所需追蹤器的數量也可能因此變多。如圖一，起始點為節點 3 (degree=5)，鄰居節點連接度最大節點為 5, 其周圍的灰色節點為追蹤器的位置。



圖一. LN_MAXDP 範例, R=2, B=2

●最小連接度節點優先挑選的布建方法**(LN_MINDP)**

- 相較於 LN_MAXDP 演算法，LN_MINDP 演算法則是由節點最小連接度開始挑選，可以有較高的機率，從網路拓撲結構的末端開始劃分出來的保護區域，可減少零散的區域的發生。

在 R 的限定條件下，允許保護區域內節點少量的增加，納入 PA 內的增加節點，以不增加追蹤器數量為原則，來對選擇追蹤器的位置進行調整，既 PA 內節點的上限為 B+F，目的在減少所需追蹤器的數量，演算法如下:

●LN_FB_MAXDP: 微調 PA 節點數量限制+最大連接度節點優先挑選的布建方法。

●LN_FB_MINDP: 微調 PA 節點數量限制+最小連接度節點優先挑選的布建方法。

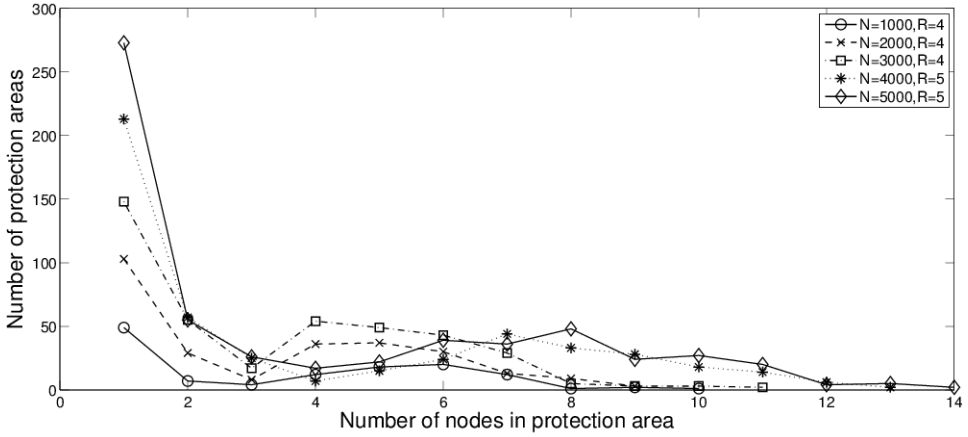
最後，我們考量網路拓撲結構保護區劃分的過程，在最後可能會變成過多零散的區域情況，形成保護區內的節點可能只有一、兩個，導致過多追蹤器保護的節點過少的節點，反而增加追蹤器所需的數量，因此我們考慮網路拓撲結構直徑的大小的因素，提出下列的方法:

●LN_FB_Hybrid 演算法

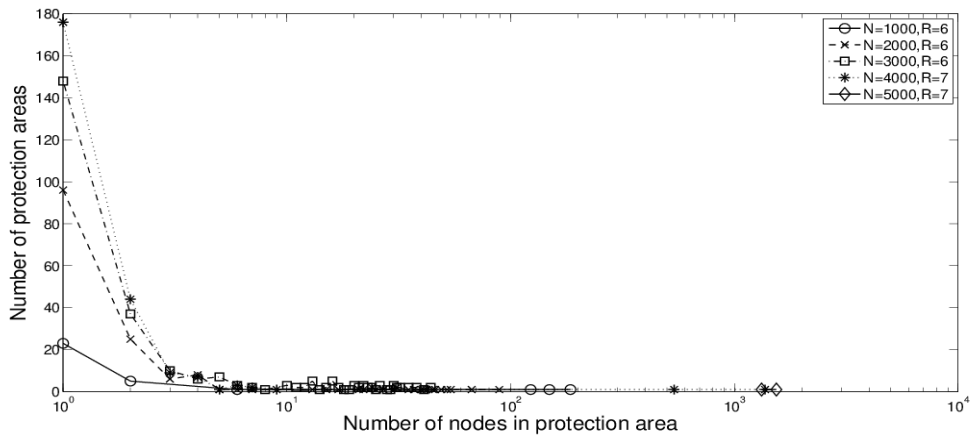
- 當要劃分保護區域時，網路拓撲結構直徑的大於 2*R 時，表示要劃分的網路範圍還相當大，在劃分新的 PA 後，網路拓撲結構還不至於出現許多零散的區域，因此以 LN_FB_MAXDP 來劃分 PA。當網路拓撲結構直徑的小於或等於 2*R 時，劃分新的 PA 後，可能會出現零散的區域情況，因此採取 LN_FB_MINDP 演算法來劃分 PA。

(b)模擬結果

我們利用 BRITE[24]隨機產生網路拓樸結構與網路資料庫 SKITTER[25]取得的網路拓樸結構，來進行模擬實驗。網路節點數量 N， N=1000～5000，各 10 張網路拓樸結構圖，，所有模擬結果皆為 10 次所得平均結果。而論文[22]的演算法我們稱為 Minimum degree placement (簡稱為 MINDP)，用來與計畫中所提出的五種方法，進行模擬比較其效能，因篇幅的限制，僅列出以 Skitter 為主的模擬結果。



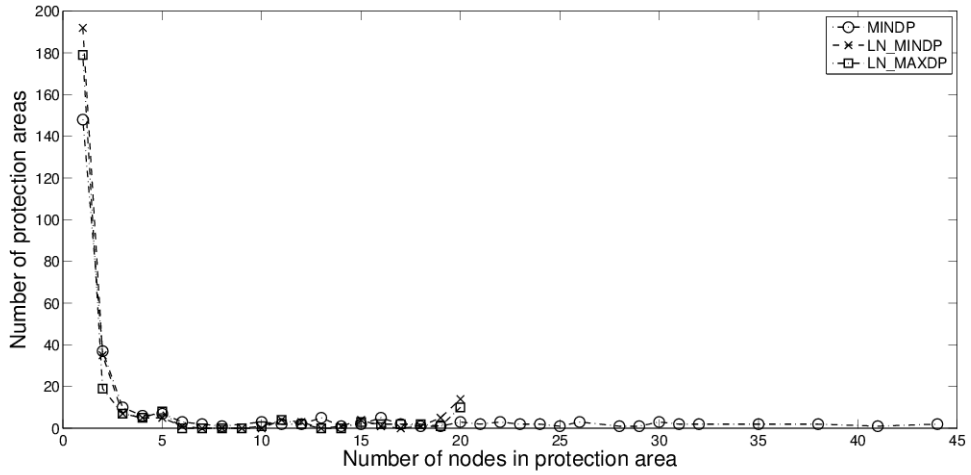
圖二. BRITE,MINDP 保護區域分佈圖(R=4,5)



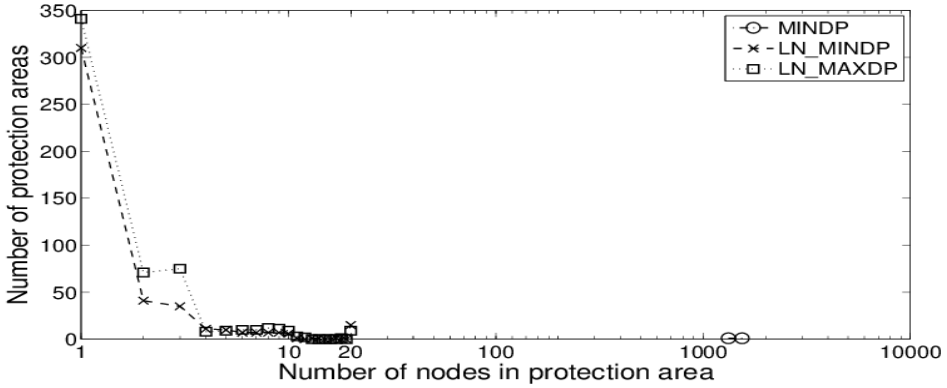
圖三. BRITE,MINDP 保護區域分佈圖(R=4,5)

BRITE 拓樸結構關係 1000 點到 3000 點最長直徑為 6，所以我們選取 R=4 來觀察，而 4000 點及 5000 點最長直徑為 7，所以我們選取 R=5。在圖二.，小範圍的 R 限制中，並不會出現保護區域節點數量過多的分佈，但是隨著拓樸結構節點數量變大，可以看見分佈區域內節點數量有逐漸增加的情況。在圖三中，我們放寬了 R 的限制，可以看到 MINDP 的方法，保護區域出現過多節點的情況。

因此，首先我們將 B 值設為 20，以所提出的劃分方法 LN_MINP 及 LN_MAXDP，來觀察保護區域節點分布情況。



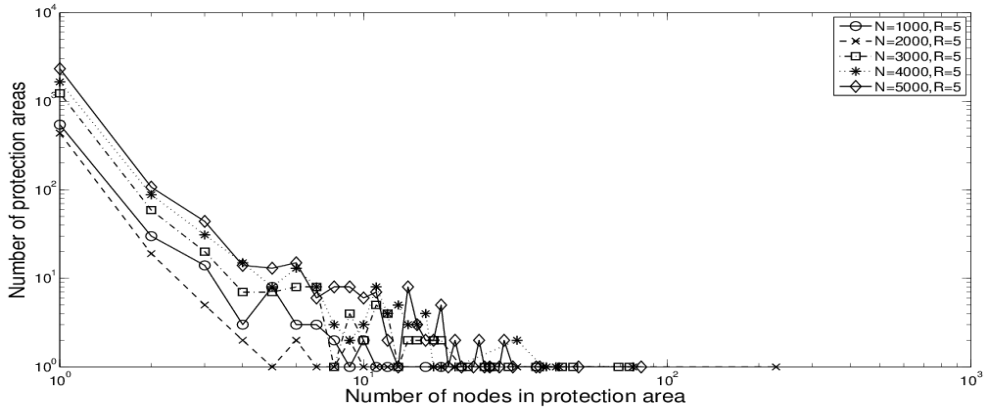
圖四. 保護區域分佈比較圖(N=3000, R=6, B=20)



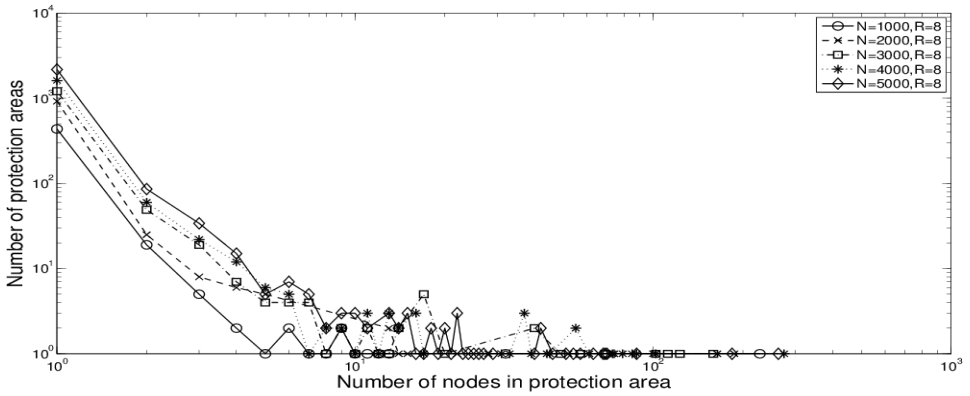
圖五. 保護區域分佈比較圖(N=5000, R=7, B=20)

由圖四、五可以看到經過限制 B 值， LN_MINDP, LN_MAXDP 可以把所有的保護區域節點數量限制在 20 之內，可避免保護區域內節點數量過多的情況發生，讓搜尋攻擊者的困難和成本花費下降。

而 SKITTER 拓樸結構最長距離都超過 20，我們先以 R=5 及 R=8 來觀察 MINDP 方法保護區域分佈情況。



圖六. SKITTER_MINDP 保護區域分佈圖(R=5)



圖七. SKITTER_MINDP 保護區域分佈圖(R=8)

在圖六與圖七中， MINDP 的劃分方法，在 skitter 的拓樸結構下，PA 出現過多的數量的情況更明顯。因此，我們設定 B 值為 20，來觀察 R 值與追蹤器數量布建成本的關係。

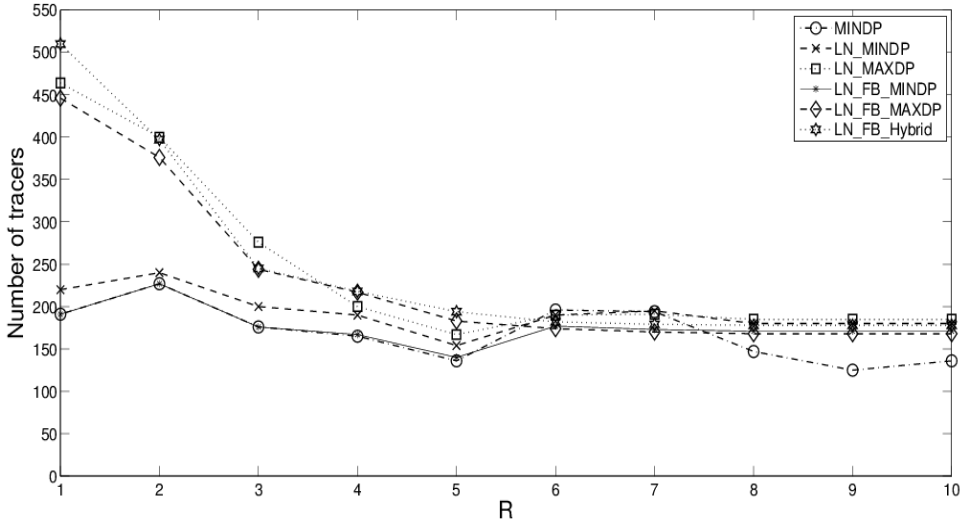


圖 八.SKITTER, 追蹤器成本比較(N=1000,B=20)

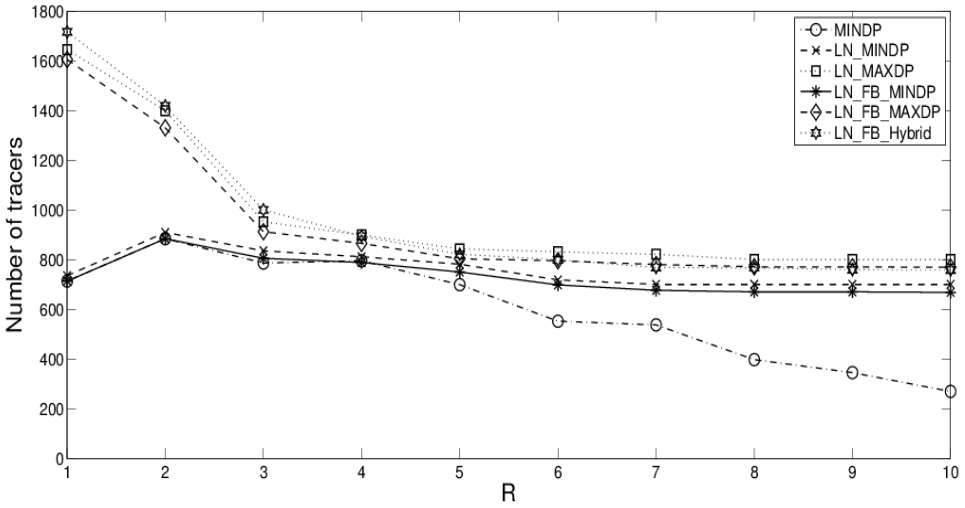


圖 九.SKITTER, 追蹤器成本比較(N=3000,B=20)

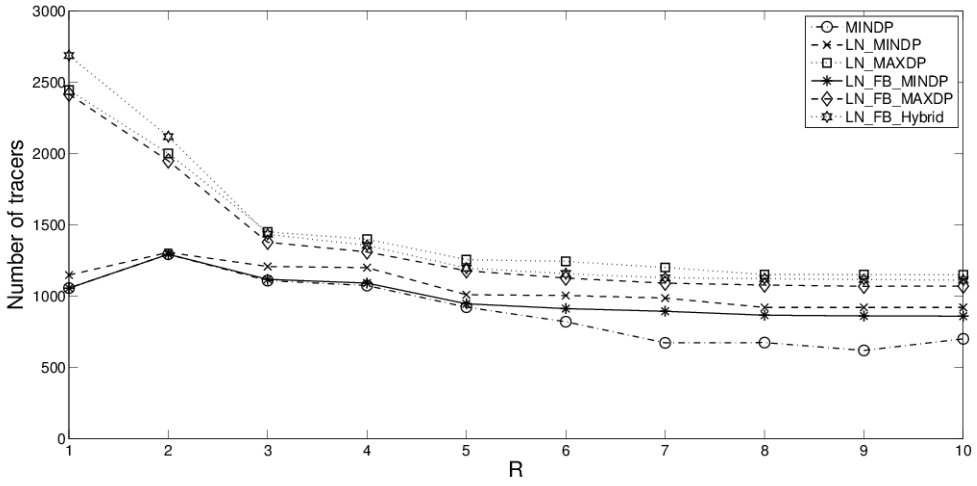
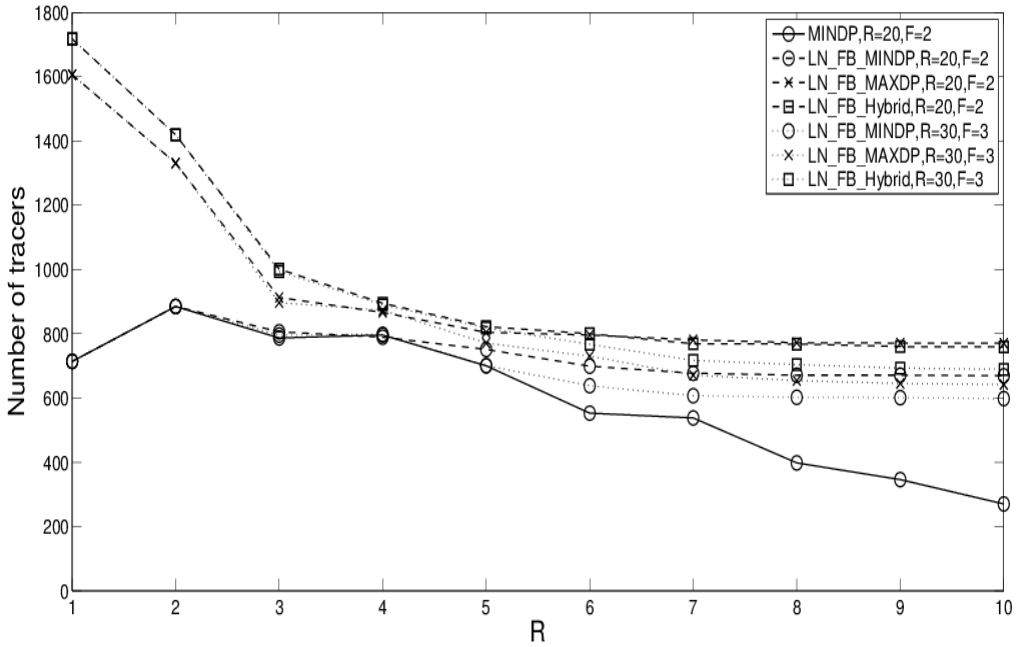


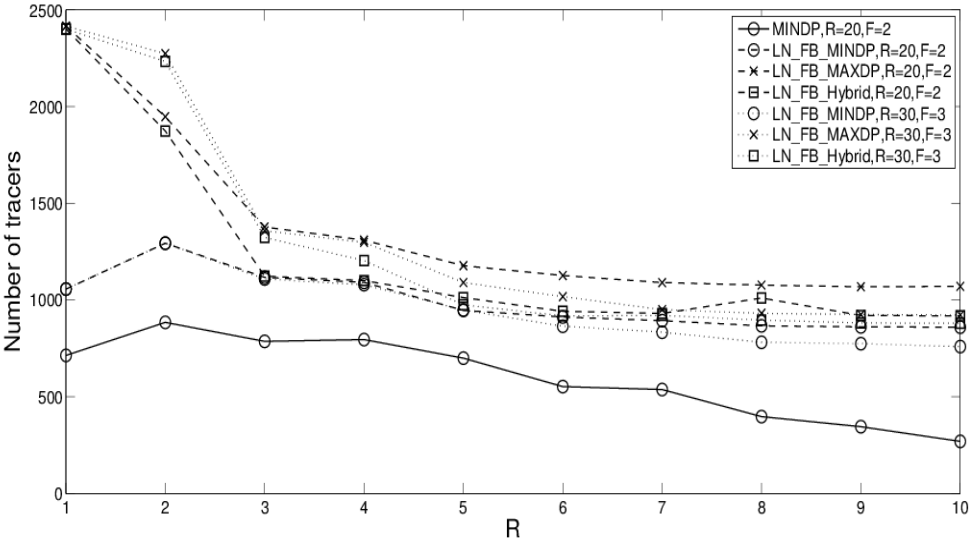
圖 十.SKITTER, 追蹤器布建成本比較(N=5000,B=20)

由圖八~圖十,為 SKITTER 拓樸結構,各演算法追蹤器成本比較圖,雖然原本 MINDP 演算法的追蹤器成本皆為最低，但必須付出的代價為搜尋攻擊者過高的成本，而我們由圖中，亦可觀察到可微調的演算法之追蹤器布建成本，略低於無微調的演算法。

事實上，追蹤器的數量與 B 值的多寡息息相關，在 SKITTER 實驗圖九~圖十中可以發現到 Bound 值設定為 20 時候，我們所提出的方法，布建的追蹤器成本大概為總節點數的三成，而 MINDP 追蹤器為兩成，因此如果假設如果追蹤器成本限定在總節點數的兩成左右話，B 值數量應為多少？換言之，以成本的考量來估算 B 值，我們可以由以下的模擬來觀察(圖十一, 圖十二)，B 值設成 30 可達此目的。



圖十一. SKITTER 追蹤器布建成本限制比較(N=3000)



圖十二. SKITTER 追蹤器布建成本限制比較(N=5000)

四、計畫自評

在本計畫中，我們提出可調整保護區域內節點數量的方法來，且可以成本的多寡，來調整保護區域內節點數量。擬結果的顯示，其中以 LN_FB_MINDP 效能較佳，且追蹤器布建的成本也接近 MINDP 的方法，但不同的是，我們可以透過 PA 內節點數量的控制，輕易地掌握攻擊來源的搜尋成本。計畫相關的研究成果，論文已發表在 *IEEE ICCT* 2011 的國際會議[26]，而計畫相關的延伸研究結果亦將整理投稿於國外期刊。本計畫原本預計兩年的時間，但只獲一年的補助，計畫雖已結束，但後續有關研究仍將持續進行。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，可培養出對防範 DDoS 攻擊認知的科技人才，以落實前瞻產業技術建立及人才培育的目標。

五、參考文獻

[1] J. Mirkovic and P. Reiher, ”A Taxonomy of DDoS Attack and DDoS Defense Mechanisms,” *ACM SIGCOMM Computer Communications Review(CCR)*, vol. 34, no. 2, April 2004, pp.39-54..

[2] R. K. Chang,“Defending against flooding-based. Distributed denial-of- service attacks: a tutorial,” *IEEE. Communications Magazine*, Volume: 40 Issue: 10, pp. 42-51, Oct. 2002.

[3] A. Belenky and N. Ansari, ”IP Traceback with Deterministic Packet Marking,”IEEE Communications Letters, vol. 7, Issue 4, April 2003, pp. 162 - 164.

[4] S. Savage, D. Wetherall, A. Karlin and T. Anderson, ”Network Support for IP Traceback,” *IEEE/ACM Trans. Net*., vol. 9, no. 3, June 2001, pp.226-37.

[5] H. Sozaki, S. Ata, I. Oka, and C. Fujiwara, ”Performance Improvement on Probabilistic Packet Marking by using History Caching,” 6th Asia-Pacific Symposium on Information and Telecommunication Technologies, APSITT 2005 Proceedings, 09-10 Nov. pp.381 - 386.

[6] L. Wu, H. X. Duan, J. P. Wu, and Xing Li, ”Improved marking model ERPPM tracing back to DDoS attacker,” Third International Conference on Information Technology and Applications, ICITA, vol. 2, July 2005, pp.759-762.

[7] U. K. Tupakula and V. Varadharajan, ”A practical 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.

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

[9] M. Muthuprasanna, G. Manimaran, M. Alicherry, and V. Kumar, ” Coloring the Internet: IP traceback,” 12th International Conference on Parallel and Distributed Systems, ICPADS 2006, Vol.1, July 2006.

[10] S. M. Bellovin, ”ICMP Traceback Messages,” IETF draft, 2000; htttp://www.research.att.com/smb/papers/draft-bellovinitrace-00.txt.

[11] Henry C. J. Lee, Vrizlynn L. L. Thing, Yi Xu, Miao Ma, ICMP Traceback with Cumulative Path, an Efficient Solution for IP Traceback, International Conference on Information and Communications Security, Oct. 2003, (Springer Lecture Notes in Computer Science, Vol. 2836, pp. 124-135, Sept. 2003).

[12] V.L.L. Thing, H.C.J. Lee, M. Sloman and J. Zhou , “Enhanced ICMP traceback with cumulative path,”*2005 IEEE 61st Vehicular Technology Conference, Volume 4*, pp. 2415 - 2419 , May-1 June 2005.

[13] J. Lee and G. d. Veciana, ”Scalable Multicast Based Filtering and Tracing Framework for Defeating Distributed DoS Attacks,” *Internation Journal of Networking Management* 2005, pp.43-60.

[14] A. C. Soneren et al., ”Single-packet IP Traceback,” IEEE/ACM Transactions on Networking, vol. 10, December 2002, pp.721-34.

[15] C. Gong, T. Le, T. Korkmaz, and K. Sarac ”Single packet IP traceback in AS-level partial

deployment scenario," IEEE Global Telecommunications Conference, vol. 3, 28 Nov.-2 Dec, 2005.

[16] W. Timothy Strayer, C. E. Jones, B. I. Schwartz, J. Mikkelson, and C. Livadas "Architecture for multi-stage network attack traceback," The IEEE Conference on Local Computer Networks, Nov. 2005.

[17] Y. N. Jing, P. Tu, X. P. Wang, and G. D. Zhang, " Distributed-log-based scheme for IP traceback," The Fifth International Conference on Computer and Information Technology, Sept. 2005, pp. 711-715.

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

[19] Chun-Hsin 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**)

[20] Chun-Hsin Wang and Yen-Chih Chiang, "Multi-Layer Traceback under the Hierarchical Tracers Deployment, " 22nd International Conference on Advanced Information Networking and Applications – Workshops, 2008. AINAW 2008, Page(s): 590 – 595.

[21] Seok Bong Jeong, Young Woo Choi, and Sehun Kim, "An Effective Placement of Detection Systems for Distributed Attack Detection in Large Scale Networks, " Lecture Notes in Computer Science, 2005, Volume 3325/2005, 204-210.

[22] Islam, M.H. Nadeem, K. Khan and S.A.; "Optimal Placement of Detection Nodes against Distributed Denial of Service Attack, " ICACC '09., Page(s): 675 – 679.

[23] K. E. Defrawy , A. Markopoulou, and K. Argyraki, "Optimal Allocation of Filters against DDoS Attacks ,"*Information Theory and Applications Workshop*, 2007.

[24] http://www.cs.bu.edu/brite/

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

[26] C. H. Wang, and D. C. Chang, "Heterogeneous Against DDoS Attacks," IEEE 13th International Conference on Communication Technology (ICCT), Jinan China, September 25-28, 2011. ((EI, NSC 99-2221-E-216 -017)

Heterogeneous Tracers against DDoS Attacks

Chun-Hsin Wang and Da Chun Chang
Department of Computer Science and Information Engineering
Chung Hua University, Hsinchu, Taiwan 30012, R.O.C.
E-mail: chwang@chu.edu.tw

***Abstract*—To solve the DoS/DDoS problems efficiently, the first things is to locate the attack origins and then cooperate the filter(s) nearby for dropping abnormal packets in time. The original routers can't provide these functions such as tracking, filtering, and etc. They have to be enhanced with additional functions to defend DoS/DDoS attacks. We refer the enhanced routers as tracers. According to the characteristic, cost and necessity of tracers, three kinds of heterogeneous tracers are selected, namely tunneling-enabled tracers, marking-enabled tracers and filtering-enabled tracers. The tunneling-enabled tracers with the lowest cost can alter the path of the passing packets to destination easily. In this paper, we study how to use tunneling-enabled tracers efficiently to forward packets to the best marking-enabled or filtering-enabled tracer for locating attack origins and filtering abnormal packets in time. Four methods are proposed and compared with the optimal solution. The fourth method with the assistance of marking-enabled tracers has the best performance of protecting network bandwidth by simulation result.**

***Index Terms*—DDoS, Tracers**

I. Introduction

The network security problems accompanied with network technology occur continuously. One of serious network security problems is Distributed Denial of Service (DDoS) ([1], [2]) attacks. The DDoS attacks pose a great threat to the Internet. They are growing rapidly and always embedded in worm-based viruses, resulting in being deteriorated internet security. They always paralyze the services which network nodes can provide and occupy the network bandwidth by sending volumes of traffic to the victim. How to defend the DDoS attacks is a challenging issue for network security problem.

The key to defend DDoS attacks is to find the attack origins and then filter attack traffic as early as possible. Because the log of attack origins can be used to be evidences for post-attack law enforcement. Besides, if the attack origins can be located on demand during the attack, the anomaly attack packets can be blocked as early as possible by co-operative filtering-enabled tracers distributed over the Internet. Therefore the network bandwidth among the attackers and its target can be prevented from being occupied by attack packets.

It is surprisingly difficult to identify attack origins due to the stateless characteristic of Internet Protocol (IP). Packet forwarding at routers is determined by the destination IP address. In general, routers without input debugging capability will not record which interface is incoming and outgoing for a packet. The origin of a packet can not be identified by the source IP address since it can be spoofed easily by the sender. Though the attack origins can be identified by hop-by-hop tracing when routers have input debugging capability, the time needed to locate the attack origins may be too long to block the anomaly traffic in time. To locate the attack origins efficiently, the function of router should be enhanced to assistance in tracing attack origins.

The IP traceback [3] technology is applied to identify the attack origins and block the attack traffic. It usually relays on enhanced routers to assist in tracing the path traversed by attack traffic and then identify the machines that directly generate attack packets. In this paper, we refer to the enhanced routers which provide tracing or filtering service as *tracers*. Many techniques for IP traceback with tracers assistance have been proposed in the literature [4-22].

According the functions of tracers used in the methods of IP traceback [4-22], the tracers can be classified into five categories as follows.

- Marking-enabled tracer [4-11]: It can mark the incoming packets with tracing information such as partial of its router address or link information. The victim may trace the attack nodes by the collection of enough marked packets.
- ICMP-enabled tracer [12-14]: It can generate ICMP traceback message destined to the same as the incoming packet with a low probability. The victim can reconstruct the complete attack path by the received enough ICMP messages.
- Logging-enabled tracer [15-18]: It can log and store the digests of packets. A single packet where it is original from can be traced by query the logging-enabled tracers over the networks. The processing load of storing the digests of packets and extra hardware cost for tracers should be considered.
- Tunneling-enabled tracer [19-21]: It can redirect packets to alternate routing path by tunneling an extra IP header on original packets.
- Filtering-enabled tracer [21-22]: It can recognize and drop abnormal packets. Filtering-enabled tracers are expected to be deployed nearby where attack origins are for the protection of network bandwidth.

To defend DDoS attacks, different functions of tracers are needed to be deployed. From the discussion of tracers as above, the tracers with function of tracking and filtering are necessary requirement. The former three kinds of tracers can be used for tracking attack origins. The marking-enabled tracers are adopted since less overhead will be added to the routers. To protect network bandwidth, filtering-enabled tracers are necessary even though cost of them is high. In addition, we

*This research is supported by the National Science Council, Taiwan, R.O.C., under grant NSC 99-2221-E-216-017-

978-1-61284-307-0/11/$26.00 ©2011 IEEE

need the tracers with the function which can redirect traffic to the marking-enabled tracers or filtering-enabled tracers. The technology of IP-tunneling can redirect traffic without changing the existing routing protocols. Fortunately, most of router are built-in the function of IP-tunneling, which can also be added by a hardware interface provided by the company such as [23] easily. In summary, three kinds of heterogeneous tracers are selected to defend DDoS attacks in this work, namely tunneling-enabled tracers, marking-enabled tracers and filtering-enabled tracers.

Under cost consideration, it is hard to upgrade all routers to be tracers in short-term. There might be only partial tracers implemented in the networks. No matter how novel IP traceback techniques are, it will be useless when attack traffic does not pass through any deployed tracers. There exists two facts which will affect the performance of defending against DDoS attacks. The first is that attack origins may not be located once the attack traffic does not pass through any tracers with function of tracking. The second is that the attack packets can not be filtered if they do not pass through any filtering-enabled tracers. Although a good placement of tracers may improve these two problems, it's not enough to solve DDoS attacks efficiently. Because the two facts may still exist when only partial tracers are deployed in the networks. This motives us to think the problem how to make attack traffic passing the deployed tracers such that attack origins can be traced and attack traffic can be filtered in time.

In this paper, we study how to use tunneling-enabled tracers efficiently to redirect traffic to marking-enabled tracers or filtering-enabled tracers to defend DDoS attacks. If abnormal packets are forwarded to their neighboring filtering-enabled tracers or marking-enabled tracers, the network bandwidth can be protected and attack origins can be tracked in time. Since the tunneling-enabled tracers have no ability to recognize which packets are abnormal, the normal packets may be redirected to longer path to destination. It results in wasting network bandwidth, especially when no attacks happen. The issue how to decide whether packets are redirected or not and the problem how to select the best forwarding candidate of filtering-enabled or marking-enabled tracers will affect the performance of protecting network bandwidth. But these problems have never been discussed in previous related work [19-22]. To protect network bandwidth, four methods are proposed and compared with the optimal solution. The fourth method by the assistance of marking-enabled tracers has the best performance by simulation result.

The rest of the paper is organized as follows. The problems of defending against DDoS attacks by heterogeneous tracers and analysis of performance are discussed in section II. The proposed methods are described in section III. Simulation results are presented in section IV. Finally, some concluding remarks and future work are given in section V.

II. The problems against DDoS attacks by heterogeneous tracers

Due to the cost consideration, only partial routers are supposed to be upgraded as tracers against DDoS attacks. Three kinds of tracers with different functions are considered, namely tunneling-enabled tracers, marking-enabled tracers and filtering-enabled tracers. Only few of routers will be upgraded to the filtering-enabled tracers due to high cost of them. The attack flow is supposed that it can be tracked by the first marking-enabled tracer which the attack traffic meets. The tracking method can be found in our previous work [11]. The cost of upgrading routers to be heterogeneous tracers in order is filtering-enabled tracers, marking-enabled tracers, and then tunneling-enabled tracers. In reality, most percentage of deployed tracers in networks will be tunneling-enabled tracers due to low cost of them. It's reasonable that the number of marking-enabled tracers is more than the filtering-enabled tracers.

Three kinds of heterogeneous tracers are supposed to be deployed randomly in networks. Since most of deployed tracers are tunneling-enabled tracers, traffic may have high probability of passing them compared to the others two kinds of tracers. To defend DDoS efficiently, tunneling-enabled tracers can be used to redirect traffic to marking-enabled tracers and filtering-enabled tracers for tracking and filtering.

The purpose of redirecting packets to marking-enabled tracers is trying to find attack origins. In fact, only a few of marked packets with tracing information are enough to trace attack origins [9]. Tunneling-enabled tracers can redirect packets to making-enabled tracers nearby in low probability. In this way, the wasting bandwidth by tunneling for tracking attack origins will be limited. Therefore we will focus on the issue how to choose the best filtering-enabled tracer which packets will be redirected to.

Comparing with the original situation which no tracers are deployed, bandwidth are expected to be protected by the assistance of tunneling-enabled and filtering-enabled tracers. Since tunneling-enabled tracers have no ability to recognize which packets are abnormal, we have two problems how to decide whether passing packets are redirected or not and how to select the best filtering-enabled tracer. To help us to analyze and solve these two problems, the object function is defined as the difference in network bandwidth consumed without tracers and with tracers.

To define the object function, some notations and definitions are given as follows.

- The tunneling-enabled tracer, T_i.
- The candidate for filtering-enabled tracer which packets will be redirected, F_i.
- The victim node, V_i
- The number of data packets passing through T_i are supposed to be D_p.
- The average length of packet, l_a.
- The shortest hop distance between any two nodes a and b is denoted by $d(a, b)$.
- The percentage of normal packets in D_p is supposed to be α. That is the percentage of abnormal packets in D_p is $1 - \alpha$.
- The probability of redirecting data packets to F_i by T_i is denoted by P_r.
- The network bandwidth occupied by normal packets and abnormal packets are B_n and B_a respectively.

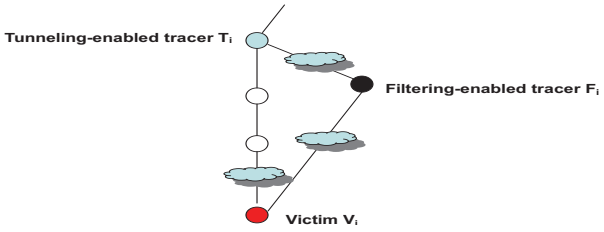


Fig. 1. Packets redirection to filtering-enabled tracer by tunneling

- The object function, $B_s(D_p, \alpha, P_r)$

From the definition as above and Figure.1, we can analyze the network bandwidth consumed by the effect of tunneling. The network bandwidth occupied by normal packets and abnormal packets can be computed respectively as follows.

- $B_n = l_a \cdot D_p \cdot \alpha(P_r \cdot (d(T_i, F_i) + d(F_i, V_i)) + (1 - P_r) \cdot d(T_i, V_i))$
- $B_a = l_a \cdot D_p \cdot (1-\alpha)(P_r \cdot d(T_i, F_i) + (1-P_r) \cdot d(T_i, V_i))$

Therefore the occupied network bandwidth with tunneling and filtering by tracers is $B_n + B_a$. we have,

$$B_n + B_a = l_a \cdot D_p(P_r \cdot d(T_i, F_i) + \alpha \cdot P_r \cdot d(F_i, V_i) + (1 - P_r) \cdot d(T_i, V_i))$$

The network bandwidth occupied by D_p from T_i to V_i is $l_a \cdot D_p \cdot d(T_i, V_i)$ without any redirection. The object function of saving networks bandwidth can be computed as follows.

$$\begin{aligned}
&B_s(D_p, \alpha, P_r) \\
&= l_a \cdot D_p \cdot d(T_i, V_i) - (B_a + B_n) \\
&= l_a \cdot D_p \cdot (d(T_i, V_i)(P_r + (1 - P_r)) - (B_a + B_n) \\
&= l_a \cdot D_p \cdot P_r \cdot d(T_i, V_i) - l_a \cdot D_p \cdot P_r(d(T_i, F_i) + \alpha \cdot d(F_i, V_i)) \\
&= l_a \cdot D_p \cdot P_r(d(T_i, V_i) - (d(T_i, F_i) + \alpha \cdot d(F_i, V_i))
\end{aligned}$$

From the object function, we can see that $B_s(D_p, \alpha, P_r)$ depend on P_r and α. When α is small, it means that the situation of attacks is serious. Let $P_r = 1$ enable tunneling-enabled tracers always works to redirect abnormal traffic to filtering-enabled tracers nearby, the saving bandwidth can be maximum. If no attacks happen (i.e., $\alpha = 1$), the redirection of packets will have no benefit because we can see that $d(T_i, V_i) \leq d(T_i, F_i) + d(F_i, V_i)$ in Figure. 1. It's hard to predict the situation what a degree of network attacks is. The value of α can not be controlled, while the probability of redirecting data packets can be controlled by tunneling-enabled tracers easily. The methods how the tunneling-enabled tracers decide whether redirect passing packets or not are proposed in the next section.

Since packets being redirected still can not be distinguished which packets are abnormal by the proposed methods, the normal packets may be redirected to alternative path. To reduce unnecessary bandwidth consumed, the difference in the length of alternative path and original path is expected to be minimum. Therefore the best candidate for filtering-enabled tracer can be selected by minimizing the difference in hop distance of path to destination with redirection and without redirection. That is to find the filtering-enabled tracer which can minimize $\{d(T_i, F_i) + d(F_i, V_i) - d(T_i, V_i)\}$.

III. Decision whether packets are redirected or not

From the discussion in previous section, packets are expected to be redirected to filtering-enabled tracers when the situation of attacks is serious. On the contrary, packets should not be redirected when no or few attacks happen. Based on this principle, four methods how to decide whether packets are redirected or not are proposed as follows.

- **All-tunneling**: All packets passing tunneling-enabled tracers are redirected to the best filtering-enabled tracer. The benefit of this method is that all abnormal packets can be filtered. Network bandwidth may be wasted when no attacks or few attacks happen.
- $50\%-$**tunneling**: The passing packets will be redirected by tunneling-enabled tracers in a half probability. It may reduce the wasting bandwidth when few attacks happen but abnormal packets may not be blocked before the victims.
- **Dynamic tunneling**: The probability of redirecting packets is updated dynamically according to the feedback from filtering-enabled tracer which packets will be redirected to. Since only filtering-enabled tracers can recognize which packets are normal, the ratio of abnormal packets to packets from each associated tunneling-enabled tracer can be computed individually. The ratio is supposed to return to its associated tunneling-enabled tracer and being used to the probability for the decision whether passing packets are redirected to or not. This method may reduce the wasting bandwidth and filter most of abnormal packets before the victims.
- **Marking assistance tunneling**: The function of marking-enabled tracers can trace attack origins. In our previous work [11], the attack origins can be traced by their first met marking-enabled tracers. The upstream tunneling-enabled tracers of the making-enabled tracers which do not find any attack origins can be turned off to reduce their overhead. The method of marking assistance tunneling is designed to turn off tunneling-enabled tracers which no attack flows will be passing through. The probability of redirecting packets is the same as dynamic-tunneling method.

IV. Simulation Results

In this section, simulations are performed to study the performance of the proposed four methods in previous section. To simulate internet topology, the real-word internet topologies from the skitter database [24] is used to generate random graphs. Each link has a cost of one hop count. The dynamic change in the configuration of routing path is not considered in our simulation. The routing table at each router is assumed to be maintained by shortest path routing algorithm. Number of nodes in the networks is from 1000 to 5000. For each data point, twenty random graphs are generated.

One hundred of number of nodes are randomly selected as attack nodes and victims are randomly selected from the others. 10000 packets are simulated for each random graph. The percentage of attack traffic is from 30% to 90%. If the

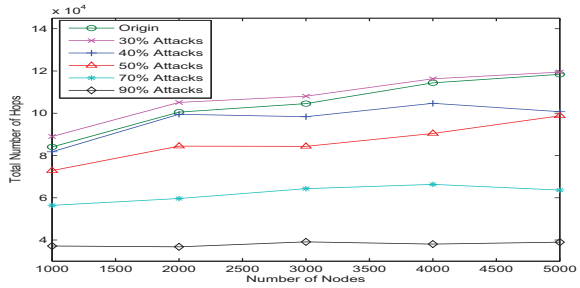


Fig. 2. All-tunneling in 80% T and 20% F

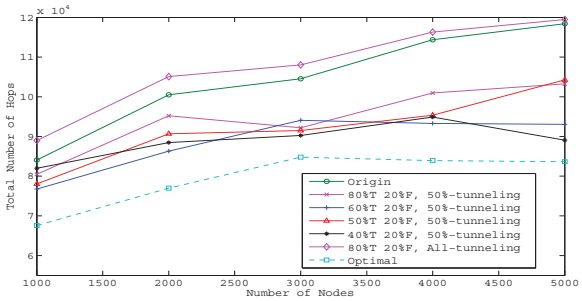


Fig. 3. 50%-tunneling in 30% attack traffic

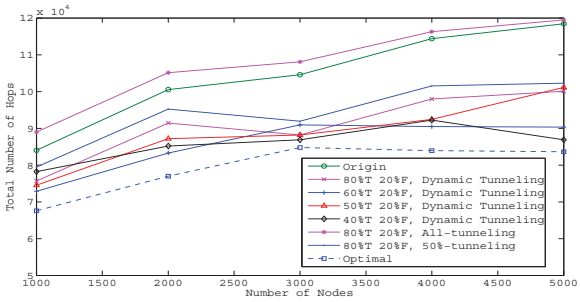


Fig. 4. Dynamic tunneling in 30% attack traffic

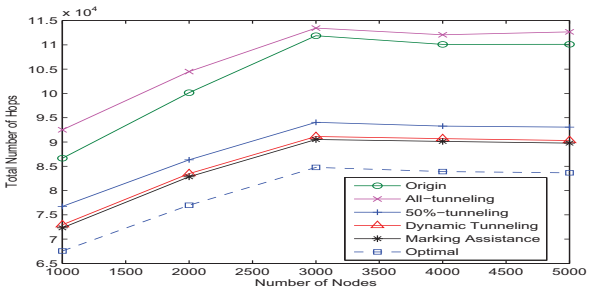


Fig. 5. Marking assistance tunneling in 30% attack traffic

percentage of attack traffic is 30%, it means that there are 3000 abnormal packets. The source node of abnormal packets are randomly selected from the 100 attack nodes.

The main performance metric is the total number of hops that packets travel paths in the networks. For the purpose of comparison, the original hop counts that packets travel paths without any redirection is measured. In addition, we also implement the optimal method which normal packets will not be redirected and abnormal packets will be redirected to the best filtering-enabled tracer.

There are three kinds of heterogeneous tracers are deployed randomly. The total number of tracers is a half of number of nodes in the networks. To show the simulation results, the notation of tracers are simplified. The tunneling-enabled tracers, filtering-enabled tracers, and making-enabled tracers are represented by "T", "F", and "M" respectively in the following figures. For example, 20%F means that twenty percentage of all tracers are filtering-enabled tracers.

Fig. 2 shows the performance of all-tunneling method when the percentages of attack traffic are from 30% to 90%. The tunneling-enabled tracers is 80% and filtering-enabled tracers is only 20% in all tracers. From this figure, we can observe that all-tunneling can redirect abnormal packets for filtering efficiently when the attack traffic is more than 40%. The performance for 30% attack is less than the original method without any redirection. This is because most of packets are normal and redirected to longer path. The wasting bandwidth is more than the saving bandwidth by filtering abnormal packets.

In Fig .3, 50%-tunneling and optimal methods are also simulated in 30% attack traffic. In the environment 80%T and 20%F, the performance of 50%-tunneling method is better than original method but still worse than the optimal method. One half of packets are redirected to filtering-enabled tracers in 50%-tunneling method. It can reduce the wasting bandwidth. There another reason that causes unnecessary redirection may be too many deployed tunneling-enabled tracers. The percentage of tunneling-enabled tracers from 40% to 60% are also simulated. From Fig .3, we can also see that the performance is improved when number of tunneling-enabled tracers is decreased. The performance gap between them and the optimal method is still large.

In Fig .4, the performance of dynamic tunneling method is better than the others but optimal method in 30% attack traffic. This because dynamic tunneling method can avoid most of unnecessary redirection of normal packets by the feedback from filtering-enabled tracer which packets are redirected to. In the environment 80%T and 20%F, the performance of dynamic tunneling method is better than 50%-tunneling method. We can also observe that the performance is improved when number of tunneling-enabled tracers is decreased. In 40%T and 20%F, the performance of dynamic tunneling method is close to the optimal method when number of nodes is 3000.

In Fig. 5, marking-enabled tracers help to turn off tunneling-enabled tracers which no attack flows are passing through. In the environment 60%T, 20%F and 20%M, the marking assistance tunneling is simulated in 30% attack traffic. From this figure, we can see that the performance of marking assistance tunneling is better than the others and the performance of dynamic tunneling is close to it. Since tunneling-enabled tracers which no attack flows are passing through can be turned off, the normal packers passing the disabled tunneling-tracers will not be redirected absolutely. Therefore unnecessary wasting bandwidth can be avoided. This is the reason why the performance of marking assistance tunneling is better than it of dynamic tunneling.

Fig. 6 shows the performance of proposed methods for different percentage of attacks from 30% to 90% in the environment 60%T, 20%F, and 20%M. The number of nodes

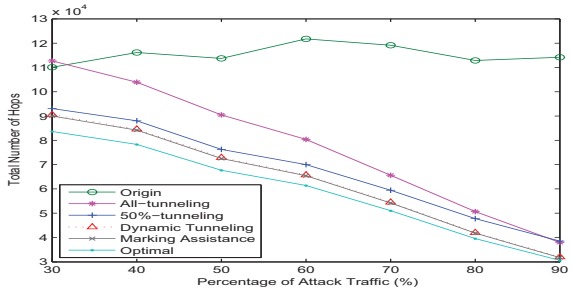


Fig. 6. Different percentage of attack traffic in 60%T, 20%F and 20%M

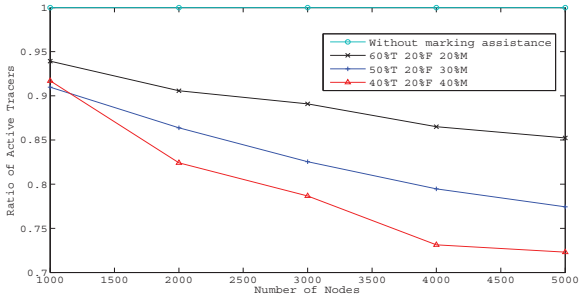


Fig. 7. The ratio of active tracers versus percentage of marking-enabled tracers

in the network is 5000. The performance of all-tunneling is worse than the original method only when attack traffic is 30%. All of the proposed methods have better performance than the original method when attack traffic is more than 30%. The performance of marking assistance tunneling is better than the others but the optimal method.

The marking assistance tunneling method not only has better performance than the other proposed method but also can reduce the overhead of tracers. By the assistance of marking-enabled tracers, tunneling-enabled tracers which no attack flows are passing through can be turned off. Fig. 7 shows that the ratio of active tracers is decreased as percentage of marking-enabled tracers is increased from 20%M to 40%M in 50% attack traffic when number of nodes is more than 2000. The probability of detecting no attack flows will be increased when number of marking-enabled tracers is increased. That is more tunneling-enabled tracers which no attack packets are passing through can be found and turned off.

V. Conclusion and Future Work

To defend DDoS attacks efficiently, three kinds of heterogeneous tracers upgraded from routers are proposed. Due to the cost consideration, there may only few of filtering-enabled tracers deployed in the networks, while low cost of tunneling-enabled tracers can be deployed easily. In this paper, we study the problem how to use tunneling-enabled tracers efficiently to redirect traffic to marking-enabled tracers or filtering-enabled tracers for tracking attack origins and filtering abnormal traffic. The marking assistance tunneling method has better performance than the other proposed methods. It can also locate attack origins and reduce the overhead of tracers. Simulation results show that much of network bandwidth can be protected even only 20% filtering-enabled tracers are deployed. In future, the placement problem of heterogeneous tracers will be considered. The issues how to guarantee that abnormal traffic could be trackable and filtered in time will be further studied.

References

[1] J. Mirkovic and P. Reiher, "A Taxonomy of DDoS Attack and DDoS Defense Mechanisms," *ACM SIGCOMM Computer Communications Review(CCR)*, vol. 34, no. 2, April 2004, pp.39-54.

[2] Rocky K. C. Chang, "Defending against Flooding-Based Distributed Denial-od-Service Attacks: A Tutorial," *IEEE Communicatin Magazine*, Oct. 2002, pp.42-51.

[3] A. Belenky and N. Ansari, "On IP Traceback," *IEEE Communicatin Magazine*, July 2003, pp.142-153.

[4] A. Belenky and N. Ansari, "IP Traceback with Deterministic Packet Marking,"IEEE Communications Letters, vol. 7, Issue 4, April 2003, pp. 162 - 164.

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

[6] H. Sozaki, S. Ata, I. Oka, and C. Fujiwara,"Performance Improvement on Probabilistic Packet Marking by using History Caching," 6th Asia-Pacific Symposium on Information and Telecommunication Technologies, APSITT 2005 Proceedings, 09-10 Nov. pp.381 - 386.

[7] L. Wu, H. X. Duan, J. P. Wu, and Xing Li, "Improved marking model ERPPM tracing back to DDoS attacker," Third International Conference on Information Technology and Applications, ICITA, vol. 2, July 2005, pp.759-762.

[8] U. K. Tupakula and V. Varadharajan, "A practical 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.

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

[10] M. Muthuprasanna, G. Manimaran, M. Alicherry, and V. Kumar, " Coloring the Internet: IP traceback," 12th International Conference on Parallel and Distributed Systems, ICPADS 2006, Vol.1, July 2006.

[11] C. H. Wang and Yen-Chih Chiang, Multi-Layer Traceback under the Hierarchical Tracers Deployment,in IEEE AINA 2008, pp. 590-595.

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

[13] Henry C. J. Lee, Vrizlynn L. L. Thing, Yi Xu, Miao Ma, ICMP Traceback with Cumulative Path, an Efficient Solution for IP Traceback, International Conference on Information and Communications Security, Oct. 2003, (Springer Lecture Notes in Computer Science, Vol. 2836, pp. 124-135, Sept. 2003)

[14] V.L.L. Thing, H.C.J. Lee, M. Sloman and J. Zhou,Enhanced ICMP traceback with cumulative path,2005 IEEE 61st Vehicular Technology Conference, Volume 4, pp. 2415 - 2419 , May-1 June 2005.

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

[16] Y. N. Jing, P. Tu, X. P. Wang, and G. D. Zhang, " Distributed-log-based scheme for IP traceback," The Fifth International Conference on Computer and Information Technology, Sept. 2005, pp. 711-715.

[17] W. Timothy Strayer, C. E. Jones, B. I. Schwartz, J. Mikkelson, and C. Livadas "Architecture for multi-stage network attack traceback," The IEEE Conference on Local Computer Networks, Nov. 2005.

[18] C. Gong, T. Le, T. Korkmaz, and K. Sarac "Single packet IP traceback in AS-level partial deployment scenario," IEEE Global Telecommunications Conference, vol. 3, 28 Nov.-2 Dec, 2005.

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

[20] A. Greenhalgh, M. Handley, and F. Huici, Using Routing and Tunneling to Combat DoS Attacks, Steps to Reducing Unwanted Traffic on the InternetWorkshop, SRUTI;05.

[21] F. Huici and M. Handley, An Edge-to-Edge Filtering Architecture Against DoS, ACM SIGCOMM Communication Review, vol. 37, no. 2, pp. 39-50, April 2007.

[22] J. Lee and G. d. Veciana, "Scalable Multicast Based Filtering and Tracing Framework for Defeating Distributed DoS Attacks," *Internation Journal of Networking Management* 2005, pp.43-60.

[23] Juniper Networks, http://www.juniper.net/

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

附件四

國科會補助專題研究計畫項下出席國際學術會議心得報告

日期：101 年 9 月 21 日

計畫編號	NSC 99 - 2221 - E - 216 - 017 -		
計畫名稱	可防禦分散式 DDoS 攻擊的異質性追蹤器布建問題之研究（II）		
出國人員 姓名	王俊鑫	服務機構 及職稱	中華大學資訊工程學系 助理教授
會議時間	2011 年 9 月 2 日 至 2011 年 9 月 4 日	會議地點	CANADA BANFF
會議名稱	The 8th International Conference on Autonomic and Trusted Computing (ATC 2011)		
發表論文 題目	Copyright Protection in P2P Networks by False Pieces Pollution		

一、 參加會議經過

此次會議地點為加拿大 banff，雖然對外的交通不是很便利，但每年仍吸引不少的觀光客，會議時間從 9/2 至 9/4，與會的學者來自許多國家，台灣與大陸的學者亦有不少人參與，系上除了我之外，還有三個同事參與，相當熱鬧。我們先飛到溫哥華再開車進入 banff。9/2 上午抵達 banff 後，先到入會場完成報到註冊手續。會場位於 banff 的一個 conference center，離住宿的旅館，大概有 5~10 分鐘的車程，有點距離。第一天晚上的迎賓宴及第二天晚上的晚宴皆於該中心舉行，地點尚可，但內容還有很大的改善空間。

二、 與會心得

會議以三至四個 sessions 同時進行，我的 session 排於 9/4 的上午，此 session 安排一個小時，有 3 篇論文，每個人的報告時間約 15 分鐘，但有一位作者缺席，所以報告的時間相當充份，session 主持人是來自對岸的學者。由於已是第三天，來聆聽的人並不多，倒是發問的問題很多，問了 5，6 個問題，報告加上回答問題的時間，超過 30 分鐘，討論相當熱絡，獲得不少寶貴意見，收穫良多。

三、 考察參觀活動(無是項活動者省略)

參與此次會議以學術性質為主，無參觀活動。

四、 建議

近年來大陸方面參加研討會的學者漸多，國內方面出國留學的學生日漸減少，因此應該鼓勵國內的博士生，參加這樣的研討會。

五、 攜回資料名稱及內容

Proceedings of the 8th International Conference on Autonomic and Trusted Computing. (紙本)。

六、 其他

感謝國科會提供的補助經費，讓本人可以參與這次的國際會議，發表論文並與會學者學術交流，受益良多。

論文接受的文件:

寄件者: atc2011@googlegroups.com
寄件日期: 2011 年 6 月 28 日星期二 上午 9:05
收件者: chwang@chu.edu.tw
副本: atc2011@googlegroups.com
主旨: ATC-2011 Status of paper 134

Dear Chun-Hsin Wang, Chuang-Yang Chiu:

First of all, thank you very much for submitting your paper to the 8th International Conference on Autonomic and Trusted Computing (ATC-2011) to be held in Banff, Alberta, Canada, Sep 02-04, 2011.

After collecting reviews, we are happy to inform you that your paper entitled

Paper ID: ATC2011-134
Title: Copyright Protection in P2P Networks by False Pieces Pollution
Authors: Chun-Hsin Wang, Chuang-Yang Chiu

has been accepted for inclusion in the proceedings to be published by Springer's Lecture Note in Computer Science (LNCS). Below, you will find attached the reports of the reviewers. Please consider the reviewers' comments carefully when preparing the final version of your paper.

The camera-ready copy of your paper is required before July 3, 2011. We are so sorry to give you only a week of time since we have extended the deadline and make the final ready very close.

ATC-2011 site at http://cse.stfx.ca/~atc2011/ provides all necessary information such as the author kit to prepare the camera-ready, and the detailed instructions for conference registration. The hotel accommodation information will be available very soon.

Please note that authors of registered papers, or at least one of them, are requested to present their work at the conference, otherwise their papers will be removed from the LNCS digital library after the conference.

Congratulations on your excellent work and we look forward to your participation in the conference.
Best regards,

ATC-2011 Program Chairs
http://cse.stfx.ca/~atc2011/

論文摘要:

Abstract. In P2P networks, the typical methods of protecting copyright files are to distribute false files with similar key words, the same file size and so on as the copyright files or publish volumes of error messages to declare the location of nonexistent copyright files. These ways lead to the difficulty in getting the copyright files for abnormal users. But these methods does not work in P2P networks such as eMule and BitTorrent with commentaries on the shared files because users can sift the true files from the false files or error location of the shared files by the commentaries. In this paper, a new technology of copyright protection by polluting pieces of files is proposed. We distribute false pieces with the same authentication keys as normal pieces but their contents are different, which is called the false pieces with authentication collision. The abnormal users will keep sharing the false pieces of copyright files they have since the false pieces can not be identified. People may have fun to download the copyright files but they can not get the correct copyright files. Due to high cost of finding authentication collision for false pieces, the way of embedding the found authentication collisions in the copyright files is also proposed. Extend simulations show approximately 100 % protection of copyright files can be reached when the associated false pieces are distributed early in time once the sharing of copyright files happened.

附件四

國科會補助專題研究計畫項下出席國際學術會議心得報告

日期：101 年 10 月 12 日

計畫編號	NSC 99 - 2221 - E - 216 - 017 -		
計畫名稱	可防禦分散式 DDoS 攻擊的異質性追蹤器布建問題之研究（II）		
出國人員姓名	王俊鑫	服務機構及職稱	中華大學資訊工程學系 助理教授
會議時間	2011 年 9 月 25 日 至 2011 年 9 月 28 日	會議地點	Jinan China
會議名稱	13th International Conference on Communication Technology (ICCT 2011)		
發表論文題目	Heterogeneous Tracers Against DDoS Attacks		

一、參加會議經過

此次會議地點為大陸山東濟南，會議時間從 9/25 至 9/28，參加的學者來自許多國家，當地大陸的學者有不少人參與。雖然有直航的飛機，但班次有限，往返的時間與會議時間，配合上有點難度，權宜之下，去程搭直航(台北桃園機場→濟南)班次，回程無直航的班機，只好由濟南飛到深圳，再轉回台灣，第一次到對岸參加研討會，感覺濟南機場有點小，機場到市區的交通不是很便利，於是搭計程車前往會場，見識到對岸計程車開車的方式，不斷的超車，猛按喇叭，沿路看到城鄉的差距頗大，令人印象深刻。此次落腳於會場的飯店，方便參加會議的各項活動，會場位於濟南市區的齊匯維景國際大酒店，會議動用了許多山東大學的學生當義工，也有很多學生來參加與發表論文，在第三天參加晚宴，藉此與參與的學者進行交流。

二、與會心得

會議以三至四個 sessions 同時進行，我的 session 排於 9/28 的上午，此 session 安排一個半小時，有 5 篇論文，每個人的報告時間約 15 分鐘，但有二位作者缺席，所以報告的時間相當充份，session 主持人是來自對岸業界的學者。來聆聽的人學生不少，發問的問題很多，報告加上回答問題的時間，超過 25 分鐘，獲得不少寶貴意見，收穫良多。會議期間，有不少學生來報告論文，雖然有些論文的品質，有待商榷，但對岸的學生，參與的程度很積極，大陸舉辦的國際性研討會也不少，學生不須出國就有很多機會參與國際性研討會，更可藉此練習如何以英文來報搞論文，雖然不是很順暢，但已達可以接受的程度，也發現有很多學生，不再是單純念稿子，也能用英文來表達自己的想法，而參與的學生也很熱烈地提出問題，讓人感受對岸學生的學習態度比我們的學生好太多，令人憂心國內的高等教育，很快可能被對岸超前。

三、考察參觀活動(無是項活動者略)

參與此次會議以學術性質為主，無參觀活動。

四、建議

近年來大陸方面舉辦國際性的研討會頗多，國內方面有點少，期望國內舉辦更多國際性的研討會，讓我們的碩、博士生，有更多機會參加這樣的研討會。

五、攜回資料名稱及內容

攜回收錄 ICCT 2011 會議論文集的 USB 隨身碟一個。

六、其他

感謝國科會提供的補助經費，讓本人可以參與這次的國際會議，發表論文並與會學者學術交流，受益良多。

論文接受的文件:

寄件者: EDAS Conference Manager <help@edas-help.com> 代理 IEEE ICCT '11 <ieeeicct2011@sdu.edu.cn>
寄件日期: 2011 年 7 月 10 日星期日 下午 8:32
收件者: Chun-Hsin Wang
副本: Da Chun Chang; ieeeicct2011@sdu.edu.cn
主旨: [IEEE ICCT '11] Your paper #1569467145 ('Heterogeneous Tracers Against DDoS Attacks') has been accepted

Dear Dr. Chun-Hsin Wang:

Congratulations - your paper #1569467145 ('Heterogeneous Tracers Against DDoS Attacks') for IEEE ICCT '11 has been accepted and you are invited to present your paper in the 2011 13th IEEE International Conference on Communication Techonologies (ICCT).

Information about registration and camera-ready preparation will be updated in the conference website later. Look forward to seeing you this September in Jinan, China.

The reviews are below or can be found at
http://edas.info/showPaper.php?m=1569467145.

論文摘要:

Abstract—To solve the DoS/DDoS problems efficiently, the first things is to locate the attack origins and then cooperate the filter(s) nearby for dropping abnormal packets in time. The original routers can't provide these functions such as tracking, filtering, and etc. They have to be enhanced with additional functions to defend DoS/DDoS attacks. We refer the enhanced routers as tracers. According to the characteristic, cost and necessity of tracers, three kinds of heterogeneous tracers are selected, namely tunneling-enabled tracers, marking-enabled tracers and filteringenabled tracers. The tunneling-enabled tracers with the lowest cost can alter the path of the passing packets to destination easily. In this paper, we study how to use tunneling-enabled tracers efficiently to forward packets to the best marking-enabled or filtering-enabled tracer for locating attack origins and filtering abnormal packets in time. Four methods are proposed and compared with the optimal solution. The fourth method with the assistance of marking-enabled tracers has the best performance of protecting network bandwidth by simulation result.

國科會補助計畫衍生研發成果推廣資料表

日期:2012/01/11

國科會補助計畫	計畫名稱: 可防禦分散式DDoS攻擊的異質性追蹤器布建問題之研究（II）
	計畫主持人: 王俊鑫
	計畫編號: 99-2221-E-216-017- 學門領域: 計算機網路與網際網路

無研發成果推廣資料

99 年度專題研究計畫研究成果彙整表

計畫主持人：王俊鑫	計畫編號：99-2221-E-216-017-
計畫名稱：可防禦分散式 DDoS 攻擊的異質性追蹤器布建問題之研究（II）	

成果項目			量化			單位	備註（質化說明：如數個計畫共同成果、成果列為該期刊之封面故事...等）
			實際已達成數（被接受或已發表）	預期總達成數(含實際已達成數)	本計畫實際貢獻百分比		
國內	論文著作	期刊論文	0	0	100%	篇	
		研究報告/技術報告	1	1	100%		
		研討會論文	0	0	100%		
		專書	0	0	100%		
	專利	申請中件數	0	0	100%	件	
		已獲得件數	0	0	100%		
	技術移轉	件數	0	0	100%	件	
		權利金	0	0	100%	千元	
	參與計畫人力（本國籍）	碩士生	2	2	100%	人次	
		博士生	0	0	100%		
		博士後研究員	0	0	100%		
		專任助理	0	0	100%		
國外	論文著作	期刊論文	0	0	100%	篇	
		研究報告/技術報告	0	0	100%		
		研討會論文	2	2	100%		
		專書	0	0	100%	章/本	
	專利	申請中件數	0	0	100%	件	
		已獲得件數	0	0	100%		
	技術移轉	件數	0	0	100%	件	
		權利金	0	0	100%	千元	
	參與計畫人力（外國籍）	碩士生	0	0	100%	人次	
		博士生	0	0	100%		
		博士後研究員	0	0	100%		
		專任助理	0	0	100%		

其他成果 (無法以量化表達之成果如辦理學術活動、獲得獎項、重要國際合作、研究成果國際影響力及其他協助產業技術發展之具體效益事項等，請以文字敘述填列。)	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，可培養出對防範 DDoS 攻擊的認知的科技人才，以落實前瞻產業技術建立及人才培育的目標。

	成果項目	量化	名稱或內容性質簡述
科教處計畫加填項目	測驗工具(含質性與量性)	0	
	課程/模組	0	
	電腦及網路系統或工具	0	
	教材	0	
	舉辦之活動/競賽	0	
	研討會/工作坊	0	
	電子報、網站	0	
	計畫成果推廣之參與（閱聽）人數	0	

國科會補助專題研究計畫成果報告自評表

請就研究內容與原計畫相符程度、達成預期目標情況、研究成果之學術或應用價值（簡要敘述成果所代表之意義、價值、影響或進一步發展之可能性）、是否適合在學術期刊發表或申請專利、主要發現或其他有關價值等，作一綜合評估。

1. 請就研究內容與原計畫相符程度、達成預期目標情況作一綜合評估

■達成目標

□未達成目標（請說明，以 100 字為限）

□實驗失敗

□因故實驗中斷

□其他原因

說明：

2. 研究成果在學術期刊發表或申請專利等情形：

論文：■已發表 □未發表之文稿 □撰寫中 □無

專利：□已獲得 □申請中 ■無

技轉：□已技轉 □洽談中 ■無

其他：(以 100 字為限)

3. 請依學術成就、技術創新、社會影響等方面，評估研究成果之學術或應用價值（簡要敘述成果所代表之意義、價值、影響或進一步發展之可能性）(以 500 字為限)

本計畫為探討如何利用異質性的追蹤器，有效地防禦 DDoS 的攻擊。在計畫中我們針對異質性追蹤器的布建問題，深入的探討布建方法對來源追蹤與過濾異常封包效能的影響，提出可依成本的多寡，來控制所劃分保護區域內節點之數量，以控管攻擊者來源的搜尋成本，雖然目前路由器尚未提升其功能成為追蹤器，但網路安全問題已不容忽視，未來提升路由器功能成為追蹤器勢在必行，本計畫的研究成果將可提供實質的參考。