群播傳輸網路系統安全之研究

林宗億　　陳宗煦　　江清泉
國防大學中正理工學院資訊科學系
{zylin, thchen, ccchiang}@ccit.edu.tw

摘要

群播傳輸(Multicast)藉由其傳輸機制，在一對多(One-to-Many)或是多對多(Many-to-Many)的通訊中，得以極有效率地傳輸聲音、影像等諸項資料，然而群播傳輸亦因採用使用者資料報協定(UDP,User Datagram Protocol)傳送資料—資料封包遺失時，傳送端不會重新傳送。於是當遭受攻擊並導致封包遺失時，將影響群播傳輸網路原有之運作效能。

為分析攻擊對運作效能的影響，本文採用NS-2(Network Simulator-2)作為模擬工具，並訂定評估運作效能的參數，再分別模擬傳送端及接收端進行攻擊的模式，藉由模擬與統計所得的數據，進一步了解，當群播傳輸網路遭受攻擊時，將會有何種程度的影響。

關鍵詞：群播傳輸、使用者資料報協定。

Abstract

Multicast distributes voice and video efficiently under one-to-many or many-to-many communication by its transport mechanisms. However, Multicast transmits data by using User Datagram Protocol which the packets lost, senders will not be re-transmit. When it is under attack and lead to packets lost, the original performance of Multicast will be affected.

In order to analyze the performance affected by attack, we use NS-2 for simulation tool. Then we define the matrix which use for evaluates the performance. So we can understand the level of influences further which take place when Multicast is under attack.

Keywords: Multicast, User Datagram Protocol.

1. 前言

隨著網際網路發展，全球資訊網(WWW, World Wide Web）亦迅速成長，為提供多樣化的服務，伺服器加入多媒體影音傳輸，然而以往所採用的傳輸控制協定／網際網路協定（TCP／IP）資料流（Data Streaming），係屬單點傳輸（Unicast），雖然能提供可靠的服務品質（QoS, Quality of Service），但由於客戶端（Client）均須與伺服器建立連結並佔用頻寬，故使用者增加，伺服器負擔即會相對增加。

因此為解決多媒體影音在單點傳輸面臨的困境，採用群播傳輸（Multicast）可有效改善伺服器負擔與頻寬需求，對於群播傳輸群組而言，傳輸一次資料，即可讓使用者均收到資料，故群播傳輸將有效改善單點傳輸佔用大量頻寬的缺點[1]，且關於群播傳輸傳送資料也已提出部分研究[2][11][12]。而群播傳輸遭受攻擊時，勢必影響原有服務品質，為使群播傳輸網路免於受到攻擊的影響，並且持續提供良好的服務，於是提出保護群播傳輸的安全方法[4][5]。

這些針對群播傳輸安全所提供的方法，雖增加安全機制，相對亦增加額外負擔。因為傳統的群播傳輸網路沒有限制使用者加入或離開群組的動作，一旦增加認證或是加密機制，在接收資料前，使用者相對需要更多前置時間，以進行傳輸或是接收群組資訊。

因此本文將藉群播傳輸運作效能參數與 NS-2 模擬軟體[9]，進一步了解無安全機制的群播傳輸，在遭受不同攻擊類型時，所受到的影響程度，並提供未來研究群播傳輸安全議題作為參考數據。

2. 相關研究

2.1 群播傳輸網路特性與安全議題

群播傳輸網路具有三種特性[2][6][7]：（1）開放的群組會員制度，（2）所有接收者均收到相同封包，（3）傳送者並非全是群組的成員。因其特性產生相關的安全問題，如圖 **1** 。

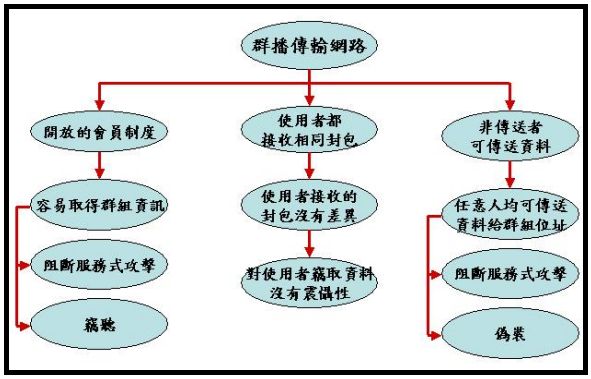

圖 1 群播傳輸特性與衍生安全議題[6]

以下分別說明各特性衍生之安全問題：

（1）開放的群組會員制度：

衍生以接收者為主的阻斷服務式攻擊（DoS, Denial of Service）以及竊聽（Eavesdropping）。對於接收者為主的阻斷服務式攻擊，須藉由控制使用者加入及離開群組的動作，以避免此類攻擊；而對於竊聽，則藉由加密群播傳輸群組，以使得攻擊者無法隨意加入群組。

（2）使用者都接收相同封包：

群播傳輸網路的傳送者對於群組接收者僅傳送一份資料，所以使用者所接收到的資料都是相同的，這是群播傳輸最大的優點之一。但也因為如此，一旦具有商業性價值的群組資料被竊取之後，由於資料並沒有任何不同，根本無法知道是被哪一位使用者所竊取的，因此沒有任何嚇阻作用（No Theft Deterrence）。若要能嚇阻使用者竊取資料，則可採用傳送的資料當中加入浮水印（Watermarking）的方式以達到目的。

（3）非使用者可傳送資料：

群播群組建立時，均會有群播群組位址，若欲傳送資料，僅需傳送至該位址，路由器即會轉送封包給相關的群組使用者，因此衍生以傳送者為主的阻斷服務式攻擊以及偽裝（Masquerading）的安全議題，對於上述攻擊方式，可藉由傳送資料前，傳送者必須經過認證，以進行防禦。

2.2 網路模擬軟體 NS-2 簡介

NS-2（Network Simulator-2）[9] 是由美國加州大學柏克萊分校（UC. Berkeley）所發展的網路模擬軟體。主要架構在 Linux 環境上，以 OTCL 和 C 語言為基礎，將模擬網路環境的結果以紀錄日誌（Trace Log）或圖表呈現。

模擬程式主要由 OTCL 語言撰寫，並結合 NS-2 的函式庫，經過如圖 **2** 的步驟，產生模擬結果。

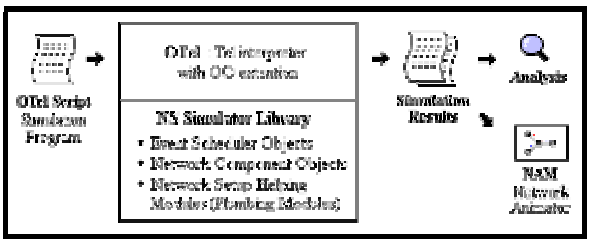

圖 2 模擬程式 NS-2 運作圖[10]

由圖 **2** 得知，由 NS-2 模擬程式產生的結果分為兩種，一是模擬紀錄日誌，另一是動畫呈現。

紀錄日誌部分，可利用資料處理軟體萃取資訊與判讀，本文則採用 AWK[2][13]作為解析紀錄日誌的軟體，由於模擬日誌所紀錄的訊息，是封包經過各個連結的時間與狀態，雖然資訊最完整，卻相當繁雜，導致使用者驗證程式的困難。

而動畫呈現部份，則能順利解決驗證程式的問題，將 NS-2 產生的結果以 NAM[8]軟體作動畫呈現，其中包含封包的傳送、丟棄等動作均能呈現。使軟體使用者得以藉由產生出來的畫面，確認模擬過程與程式，是否按照所設計的網路環境運作。

NS-2 模擬軟體的特色在於將程式模組化，將網路中各種不同的要素，諸如傳輸協定，路由協定與佇列策略等等，均設計成模組。而因為採用模組化的方式，使用者得以輕易的加入自行設計的模組並進行模擬。

3. 系統架構與模擬環境

3.1 群播傳輸效能評估系統架構

群播傳輸效能評估系統架構區分為數個流程，如圖 **3** 。

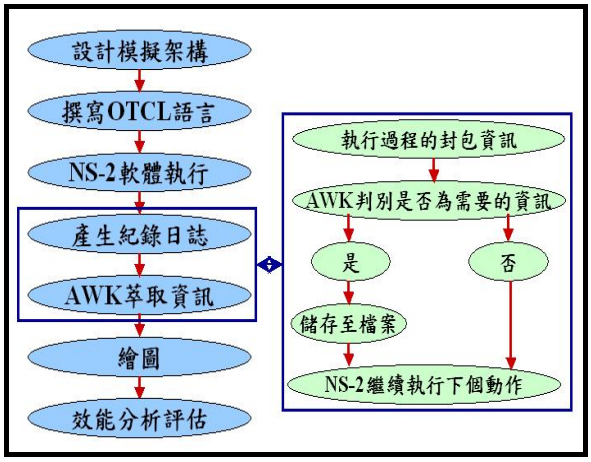

圖 3 群播傳輸系統效能評估流程圖

模擬軟體的作業環境為 Ret Hat Linux 9.0，所需安裝的軟體與版本資料如表 **1** 。

表 1 模擬群播傳輸網路效能評估軟體需求表

所需軟體	軟體版本
NS-2	2.27
NAM	1.10
AWK	RetHat Linux 9.0 內建

3.2 群播傳輸網路攻擊模式探討

本文針對群播傳輸於協定設計上，可能遭受的各種攻擊行為，探討傳送者與接收者身分進行攻擊的模式。

（1）傳送者攻擊模式探討：

以傳送者攻擊模式而言，可由攻擊速度與攻擊

者數目兩方面，分別模擬兩者之攻擊行為與調整參數，以了解其影響程度。

（2）接收者攻擊模式探討：

以惡意接收者攻擊模式而言，可由單一接收者加入不同數目的群組，與不同數目的接收者加入同一群組兩方面，分別模擬兩者之攻擊行為與調整參數，以了解其影響程度。

並分別針對上述兩者之攻擊參數，調整模擬骨幹網路間的佇列（Queue Size）大小，以了解佇列對攻擊行為與程度的影響。

3.3 紀錄日誌效能評估參數分析

為評估群播傳輸運作效能，因此訂定如表 **2** 的效能評估參數表。

表 2 運作效能評估參數表

項次	評估項目名稱
一	群組接收者接收到的群播封包總數
二	丟棄的封包總數目
三	整體延遲時間
四	群播傳輸封包被傳送的總次數

（1）群組接收者接收的封包總數目：

評估模擬時間內接收者所收到的封包總數目（Total Number of Packets），衡量群組的運作效能，在遭受攻擊時，封包總數將有所變化。故當封包總數愈多時，即代表運作效能愈好，有關接收封包總數目的定義與統計圖例，如圖 **4** 。

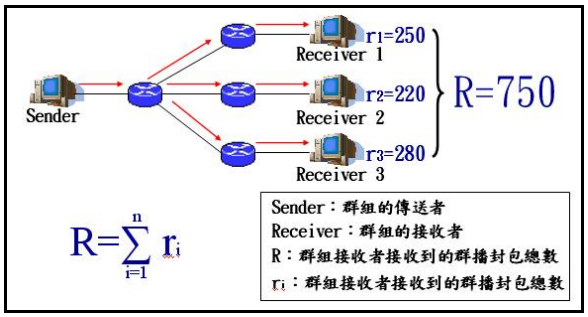

圖 4 群組接收者接收的封包總數示意圖

（2）丟棄的封包總數目：

丟棄的封包總數目定義為：統計模擬時間內被丟棄的封包數目。在遭受攻擊時，將可能使得網路壅塞而導致封包丟棄，故當丟棄的封包數目愈多，即表示運作效能愈低。

（3）整體延遲時間：

整體延遲時間定義為：群組傳送者送出第一個封包，直到接收者接收到最後一個群播群組封包的時間，稱之為整體延遲時間，如圖 **5** ，單位為秒。

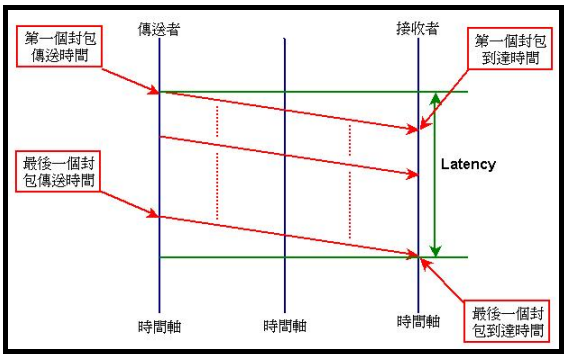

圖 5 群組整體延遲時間示意圖

（4）群播封包被傳送的總次數：

群播封包被傳送的次數定義為：封包被模擬網路中的節點轉送到下個節點時，次數加一；總次數則是每個群播封包被傳送次數的總計，如圖 **6** 。

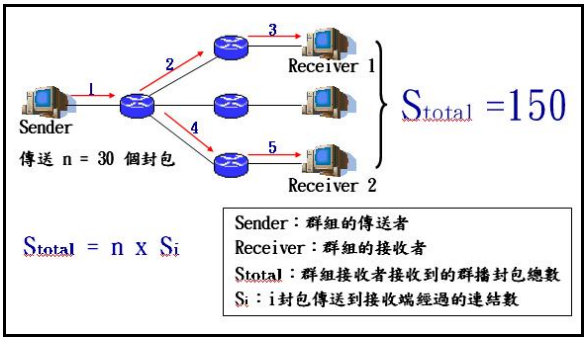

圖 6 群播封包被傳送總次數示意圖

4. 系統分析與效能評估

4.1 模擬網路環境架構與參數設定

進行群播傳輸的攻擊模擬前，必須先行設定模擬網路的環境參數，諸如節點數目、背景流量與連結頻寬等，依表 **3** 循序訂定模擬的環境參數。

表 3 網路模擬環境基本參數表

項次	參數名稱
一	模擬時間
二	網路節點數目與連結頻寬
三	節點間佇列大小（Queue Size）
四	流量（Traffic）

（1）模擬時間、網路節點數目與連結頻寬：

訂定模擬節點數目為 100 個，並考量群播傳輸乃以骨幹網路為主，故頻寬定為 45MB，繪製網路拓樸圖，如圖 **7** 。而模擬執行時間，則考量記錄

日誌檔案與後續分析，設定為一分鐘。

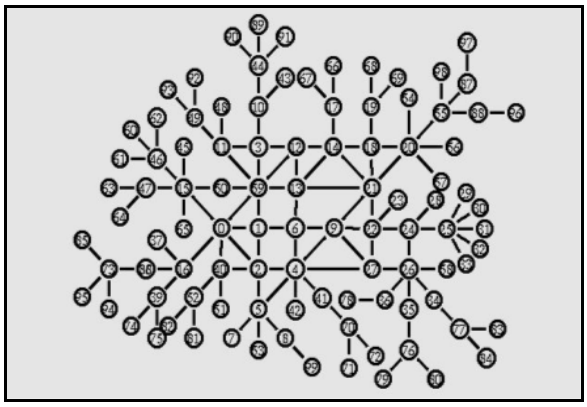

圖 7 模擬網路架構拓樸圖

（2）節點間佇列設定與背景流量：

為使模擬環境能較符合實際網路狀況，訂定此兩者參數，並且未受攻擊前，其封包丟棄率不會過高。因此在三個群播群組的模擬網路，如表 **4** 。模擬在不同負載及佇列下，統計其丟棄封包總數目與群組接收封包總數目，如圖 **8** ，圖 **9** 。

表 4 群播群組成員資訊表

群播群組	傳送者節點	接收者節點
第 1 組	93	43、14、97、28、35、71、5、52、63
第 2 組	83	46、44、68、96、32、80、70、51、39
第 3 組	73	11、66、20、29、27、84、99、42、40

由圖 **8** ，圖 **9** 得知在不同負載下，隨著佇列漸增，被丟棄封包減少，而接收封包增加；並且隨著背景流量的負載度漸增，亦相對使得被丟棄封包增加，而接收封包則減少。本文訂定背景流量為中負載，佇列為 5，作為模擬網路中的預設值。

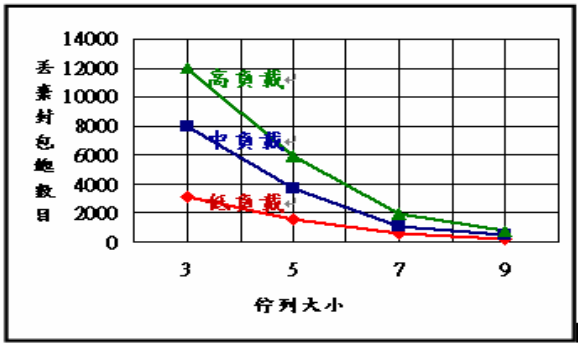

圖 8 不同佇列與負載下，丟棄封包總數目圖

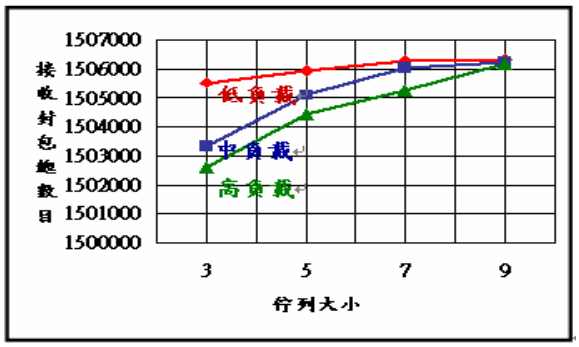

圖 9 不同佇列與負載下，群組接收封包總數目圖

4.2 以傳送者身分攻擊模擬群播網路

本文分為三個方向進行以傳送者身分攻擊的模擬，鎖定攻擊第一組，模擬並分析結果如後：

（1）單一攻擊者，調整攻擊速度攻擊分析：

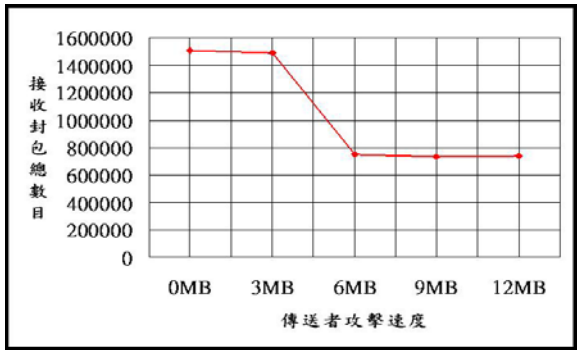

圖 10 增加攻擊速度，群組接收封包總數目圖

由圖 **10** 得知，節點之間頻寬雖為 45MB，但攻擊速度為 6MB 時，就足以使得群播傳輸接收封包降為原本的 50%左右。

（2）增加攻擊者，固定攻擊速度攻擊分析：

本文設定攻擊者攻擊速度均為 1MB，主要了解攻擊者數目越多的情況下，對於運作效能的影響。

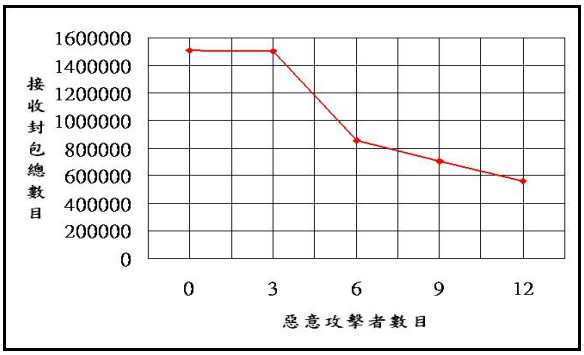

圖 11 增加攻擊數目，群組接收封包總數圖

由圖 **11** 得知，隨著攻擊者數目越多，使接收的封包總數減少，並在攻擊者數目 6 個時，攻擊影響急遽增加，由於攻擊速度均為 1MB，亦即是攻擊行為的總流量頻寬均為 6MB，所以與單一攻擊者速度 6MB 時對群組效能產生嚴重影響的現象相同。

（3）傳送者攻擊因佇列不同產生影響分析：

本文分別針對傳送者攻擊群組影響運作效能的參數，分別為攻擊速度為 12MB 與攻擊者數目 12 個，調整節點間佇列，以了解佇列對於攻擊的影響。

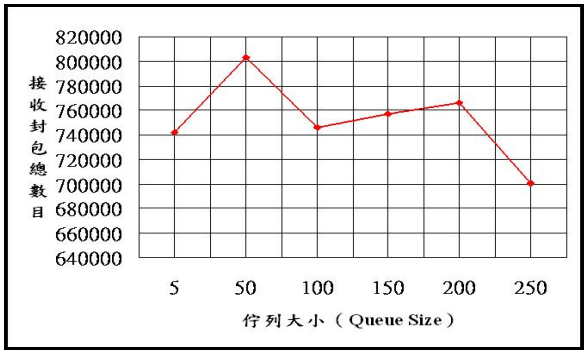

圖 12 攻擊速度 12MB 變更佇列，接收封包總數圖

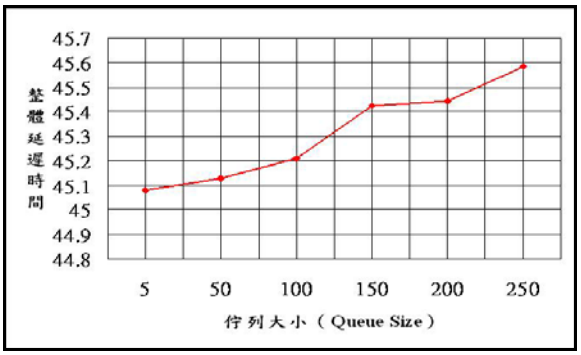

圖 13 攻擊速度 12MB 變更佇列，整體延遲時間圖

由圖 **12** 得知，單一攻擊者攻擊速度 12MB，佇列為 50 時，接收封包總數明顯提高，之後逐次提高佇列，反而使接收總數減少，係當佇列越大時，原本被節點丟棄的攻擊封包，反而能夠傳送到其他節點，導致攻擊的擴散影響。

由圖 **14** 得知，12 個攻擊者攻擊速度 1MB 情況下，雖然隨著佇列增加，接收封包總數隨之提高，但因為攻擊者數目眾多，在提高其佇列後，仍舊較單一攻擊者攻擊速度 12MB，接收的封包總數為少。

並且由圖 **13** ，圖 **15** 得知，調整佇列雖能使接收封包總數提升，但相對群組的整體延遲時間卻逐漸變長，意味著接收者接收所有封包需花費的時間變長，即代表運作效率因而降低，故調整佇列不一定能解決攻擊的影響。

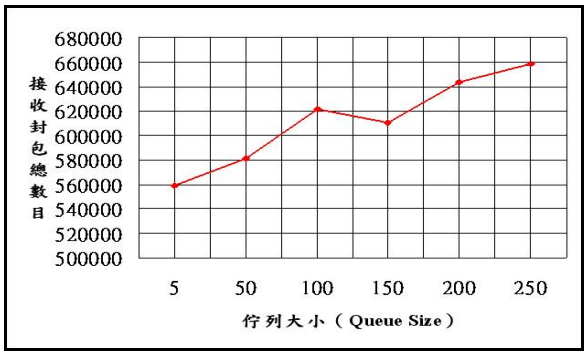

圖 14 攻擊者 12 個變更佇列，接收封包總數圖

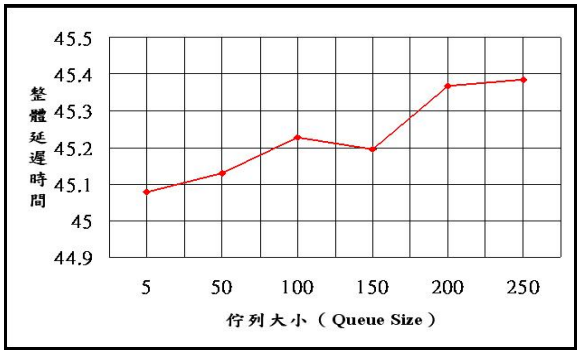

圖 15 攻擊者 12 個變更佇列，整體延遲時間圖

然而由圖 **12** ，圖 **14** 呈現的結果，即使增加佇列，接收的封包總數仍舊僅維持在原本的 50% 左右，並且增加佇列時，亦會使原本會被丟棄的攻擊封包成功傳送，進而更加影響網路的負擔。

4.3 以接收者身分攻擊模擬群播網路

本文分為三個方向進行以接收者身分攻擊的模擬，並分析結果如後：

（1）單一接收者加入不同群組數目之分析：

統計單一接收者加入不同數目的群組，群播封包被傳送的次數，如圖 **16** 。

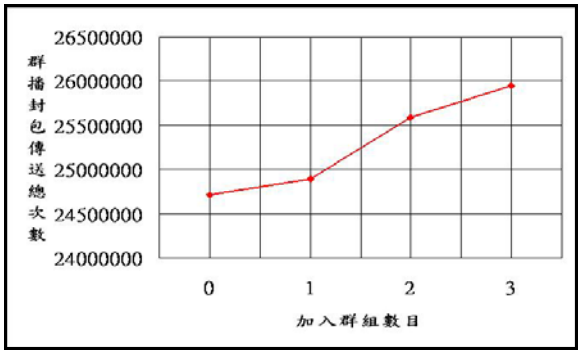

圖 16 加入不同數目群組，群播封包總次數圖

接收者加入群組越多，因為網路必須傳送這些增加的額外封包，所以群播封包被傳送的次數越增加。且對接收者而言，僅需要加入群組，便可使網路傳送額外的群播封包。

（2）增加單一群組的接收者數目攻擊分析：

由圖 **17** 中，得知接收者數目在 6 到 12 個之間，被傳送總次數成長逐漸趨緩。因為群播傳輸新增接收者時，為傳送封包給使用者，將新增必要路由器（節點）作為群組通訊。

所以當接收者數目在網路中所佔比例越來越高時，便越無需新增節點。而由於群播封包被傳送的次數定義為每個封包經過的連結數總計，所以群播封包被傳送的總次數，會隨著群組接收者增加時而增加，但增加幅度逐漸減緩。

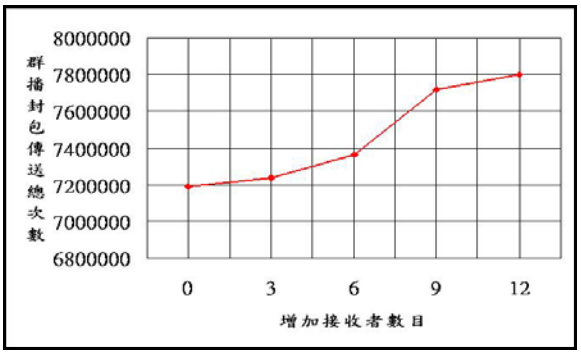

圖 17 增加群組接收者，群播封包傳送總次數圖

5. 結論

本研究以 NS-2 軟體作為模擬的工具，並提出群播傳輸效能評估的模擬系統。藉由模擬群播傳輸攻擊，與分析系統產生的紀錄日誌，進一步了解運作效能與攻擊行為的關係。採用模擬的優點在於無需多項網路設備即可實現，亦可節省收集資訊的時間，更不會因攻擊行為導致網路癱瘓。

從傳送者攻擊模擬部份而言，在骨幹網路頻寬 45MB 時，攻擊總流量僅需 6MB，即可達到顯著的攻擊效果，並使得接收封包總數降為原本的 50%左右。

另外在攻擊總流量 12MB 的情形下，即使增加佇列，能使封包的接收總數增加，但效能提升的部分相當有限，因為佇列的增加，亦相對使得群組的整體延遲時間變長。

從接收者攻擊模擬部份而言，由於群播群組對於接收者加入的動作，並無任何限制，所以接收者可以隨意的加入任何群組。而在加入群組後，若網路中具有一或多數惡意接收者，為了傳送群播封包將佔用網路的資源，雖然群播傳輸在多對多的傳輸極有效率，但其資料多屬影音傳輸，故若某網段的使用者遭到策反，進而加入許多群播群組中，將輕而易舉的癱瘓網段其他正常的通訊行為。

整體而言，本文經過各項攻擊模擬，並且針對各項效能評估參數作有系統的評估分析，可以了解攻擊行為對群播群組的影響程度，並希望提供網路管理人員在架設群播網路上作為參考。

參考文獻

[1] 胡泉基、江清泉。2001。群播傳輸實驗網路之效能評估。國防大學中正理工學院電子工程研究所。桃園。

[2] 中央研究院計算機中心，ASPAC 計畫，Overview of AWK, http://phi.sinica.edu.tw/aspac/reports/94/940111/ch1.html.

[3] Ballardie, T., and Crowcroft, J., “Multicast-Specific Security Threats and Counter-Measures,” Network and Distributed System Security, Vol. 16-17, pp.2-16, Feb., 1995.

[4] Boudani, A., and Cousin, B., “SEM: A New Small Group Multicast Routing Protocol,” *Telecommunications*, Vol. 1, pp.450-455, 2003.

[5] Judge, P., and Ammar, M., “Gothic: A Group Access Control Architecture for Secure Multicast and Anycast,” *IEEE INFOCOM*, 2002.

[6] Judge, P., and Ammar, M., “Security Issues and Solutions in Multicast Content Distribution: A Survey,” IEEE Network, January/February, 2003.

[7] Kruus, S. P., and Macker, P. J., “Techniques and Issues in Multicast Security,” Military Communications Conference, Vol. 3, pp.18-21, Oct., 1998.

[8] NAM, Network Animator, http://www.isi.edu/nsnam/nam/, July, 2002.

[9] NS-2, http://www.isi.edu/nsnam/ns/, 2002.

[10] NS-2 by Example, http://nile.wpi.edu/NS/, 2002.

[11] Rodriguez, P., and Biersack, E. W., “Continuous Multicast Push of Web Documents over the Internet,” IEEE Network, Vol. 12, No. 2, pp.18-31, 1998.

[12] Shin, M. K., and Lee, J. T., “Web-Base Real-Time Multimedia Application for the MBone,” INET 98 proceedings, 1998.

[13] The AWK Manual, Edition 1.0, Close, B. D., Robbins, D. A., Rubin, H. P., Stallman, R., and OOstrum, V. P., http://www.cs.uu.nl/docs/vakken/st/nawk/nawk_toc.html.1995.

[14] Wu, J. J., Hu, C. C., Yuan, C. K., and Chiang, C. C., “The Implementation and Performance Evaluation of Dynamic Adaptive Multicast WWW System,” Journal of Internet Technology, Vol. 1, No. 2, pp.41-49, 2000.