Detection and Prevention of DDoS Attack over Wireless IPv6 Network

林政穎* 黃永銘* 陳麒元** 曾龍*
興國管理學院資訊科學系* 國立東華大學電機所**
{b911100756, b911010096}@std.hku.edu.tw
justin@style.dj
btseng@mail.hku.edu.tw

摘要

「分散式阻斷攻擊」Distributed Denial of Service (DDoS)攻擊，是現今 IPv4 網路具有嚴重性的威脅。新一代 IPv6 網路由於具有龐大位址空間以及 IPSec 機制，因此 IPv6 網路比傳統 IPv4 網路具有更高的安全性，但 IPv6 網路上仍無法免除 DDoS 攻擊。在邁向 Wireless 及 3G 的時代，IPv6 扮演著重要的角色，而安全性也是必須被重視的一個環節。為了瞭解無線 IPv6 網路上的安全性問題，本文提出並分析 Wireless IPv6 Network 上的 DDoS 攻擊，同時我們以 Signature-Based Detection 技術進行偵測，並提出 Auto-Response Algorithm 實作 Inline IPS。就我們所知，現有文獻中尚無詳細記載 DDoS 在無線 IPv6 網路上的攻擊分析與偵測文件，本文特別針對 Wireless IPv6 Home Network，進行 DDoS 攻擊的偵測與防禦。我們以 tunnel broker 為基礎實作出 W6SGW(Wireless IPv6-enabling Security Gateway)，並規劃 Scenario-Based Testing 進行 DDoS 攻擊測試，且利用 W6SGW 來偵測並加以阻擋此攻擊。實驗結果顯示 W6SGW 可正確無誤地偵測 4to6 DDoS 攻擊。

關鍵字：DDoS，Wireless IPv6 Network，W6SGW(Wireless IPv6-enabling Security Gateway)

Abstract

Although many proposals of detection and prevention technologies for DDoS (Distributed Denial of Service) attack, it is still the major threat in IPv4 network. Due to providing larger address space and ipsec, IPv6 network is believed to be more secure than IPv4 network. However, IPv6 network still suffer from DDoS attack. In the era of the 3G and Wireless network, IPv6 plays an important role and then the security of IPv6 is important issue should be studied. In this paper, we present the security analysis of DDoS attack in the Wireless IPv6 Network and implement an integrated Security Gateway W6SGW(Wireless IPv6 enabled Security Gateway).

Our W6SGW is designed with an IPv6 active inline IPS engine, which is based on signature-based detection and auto-response algorithm. We also employ tunnel broker mechanism to implement the W6SGW (Wireless IPv6-enabling Security Gateway). To test the effectiveness of our W6SGW, we conduct scenario-based testing based on 4to6 DDoS attack over Wireless IPv6 Home Network. Our primary results show that 4to6 DDoS attack can be correctly detected and prevented by our W6SGW. To our knowledge, this is the first literature to discuss the detection and prevention of DDoS attack in Wireless IPv6 Network.

Keywords：DDoS，Wireless IPv6 Network，W6SGW(Wireless IPv6-enabling Security Gateway)

1. Introduction

在網際網路蓬勃發展下，IP 位址的需求量大增，現行使用之 IPv4 位址預計將於近幾年內耗盡，加上 Wireless 技術的發展以及 3G 產業的到來，傳統 IPv4 已無法滿足需求，推動新一代協定 IPv6 [1] 乃成為建設發展當務之急。2002 年 4 月，我國更將 IPv6 之發展列為國家六年國建計畫（旗艦計畫），展示全力發展的決心。

在 IPv6 的時代裡 3G 對 IPv6 的需求更加重要，因為目前 2.5G GPRS 與 3G R99/R4 由於 IPv4 位址不足，仍採用 NAT 技術，破壞了網路端點到端點的特性以及缺少固定 IP、Always-on，限制了 Mobile IP、VoIP 等應用的發展，然而在 3G R5 已經確定使用 IPv6 Network，由此可知 IPv6 對 3G 的重要性。

另外，在寬頻普及、WLAN 技術成熟化以及數位電視和數位廣播陸續開播等因素催化下，將帶動家庭視聽及娛樂產品的數位化和網路化風潮，使得 Home Network 更是蓬勃發展，而 Home Network 最重要的需求，即為需要足夠的 IP 位址空間，這樣才能使得大量的家電用品均可分配到 IP 位址，否則只能透過 NAT 的方式等技術來實現，但這樣將會限制 Home Network 的成長。於是擁有廣大位址空間的 IPv6 Home Network 將會是未來發展的趨勢。DLNA (Digital Living Network Alliance)在 2004 年六月的白皮書裡指出 IPv6 將納入 2005 年以後的架構裡

[7]，由此可知 IPv6 對於未來 Home Network 的重要。

此外，根據 In-Stat/MDR 於 2002 年 10 月底發表的研究報告，無線區域網路（Wireless local area network, WLAN）的技術標準 Wi-Fi 將引領無線家庭網路（Wireless Home Networking）的風潮，越來越多家庭利用 Wi-Fi 技術，將家中的個人電腦與視聽娛樂設備連結在一起。Wireless Home Network 用戶將透過 Home Gateway 的方式使各種家電產品如電視、電話、電腦等連上 Internet。由上述趨勢可知，Wireless IPv6 Home Network 將在 Digital Home Network 扮演重要角色，因此具有安全防護機制的 IPv6 Home Gateway 將會是未來重要的發展方向。

在傳統 IPv4 的網路中，分散式阻斷服務（Distributed Denial of Service）攻擊是威力強大的網路威脅[8]，也是當前網際網路相當嚴重的安全問題。2000 年年初，Yahoo、Amazon、CNN、eBay 被分散式阻斷服務(Distributed Denial of Service：DDoS)的手法攻擊，造成網站數小時的停擺與經濟上不少的損失。在以往的研究中[4]指出，現今 IPv4 與 IPv6 共存的時代下，DDoS 攻擊仍會在 IPv4 的網路架構下透過轉換機制對 IPv6 網路進行攻擊，如 4to6 DDoS 攻擊。過去 IPv6 安全性的探討多為 Wired Network，本文則提出無線 IPv6 網路上 DDoS 攻擊的安全性分析，並實作出 W6SGW(Wireless IPv6-enabling Security Gateway)來偵測及防禦無線 IPv6 網路上的 DDoS 攻擊。

本文的主要目地是研究無線 IPv6 網路上 DDoS 攻擊的安全性分析及其偵測與防禦。本文其餘內容如下，第二節討論 IPv6 網路上的安全性問題；第三節說明 DDoS 的攻擊模式與分析；第四節是我們自行開發的 W6SGW 所使用的偵測與防禦技術；第五節則是利用 W6SGW 規劃一個測試環境以進行 Scenario-Based Testing，最後是我們的結論與未來研究方向。

2. Remarks on IPv6 Security

傳統 IPv4 網路協定已經使用多年，各式各樣的網路技術與攻擊手法不斷推陳出新。雖然過去已有許多學者對於 IPv4 的安全性進行深入的研究，但網路上仍是存在著許多威脅。爲了解決 IPv4 安全性問題，新一代 IPv6 設計之初對於安全性部分已有所增強，如位址空間的擴增，IPv6 的位址長度由 32bits 擴大到 128bits，因此可以分配的位址數量大幅擴充，這樣除了可供給更多的 IP 位址空間外，也可導致駭客利用相關掃描技術與工具進行弱點掃描的難度大幅增加。

安全問題始終是與 Internet 相關的一個重要話題。由於在 IP 協定設計之初沒有考慮安全性，所以封包傳送時容易被偽造 IP 位址和修改其內容、以及在傳送過程中以 Sniffing 攔截並查看封包內容。也因此 IPv4 網路上無法保證所接收到的封包資訊是否為起始發送方和原始資料，以及資料在傳輸途中是否有被他人看過內容。有鑑於此，IPSec 的設計上可以為 IPv6 網路環境下的資料傳輸提供有效地保護及傳輸上的安全。它採取的具體保護形式包括提供傳送、接收端做資料的認證、完整性、存取控制，以及機密性等安全服務。

IPv6 雖然具有一些增強的安全性機制，但 IPv6 協定仍具有許多安全的挑戰，特別是 IPSec 目前在主要的作業系統並未強制性要求，因此，IPv6 上的安全性問題也是相當值得我們探討的。在[4]文中提到 IPv6 現階段安全性問題最大的部份在於 IPv4/IPv6 間的轉換機制。為了讓 IPv6 與 IPv4 環境共存，目前已提出 Dual-Stack、Tunnel Broker[2]、ISATAP[6]、6to4[3]等數種轉換機制使 IPv6 網路與 IPv4 環境相互運作。以 Dual-Stack 同時共存 IPv4/IPv6 的雙堆疊機制來說，目前 IPv 6 堆疊也仍未完全支援 ipsec，所以 IPv6 轉換機制仍存在一些尚未被深入研究的安全威脅。也由於這些不同轉換機制在架構上缺乏完整的安全性考量，再加上仍有許多來自上層通訊協定的安全性威脅等問題存在，而造成有些攻擊是透過 IPv4 攻擊 IPv6[4]，因此，除了 IPv6 網路本身的安全性外，由 IPv4 所延伸至 IPv6 上的安全性也是我們需要加以研究的主題。

在 P.Savola 與 C.Patel[10]的研究中指出，由於 6to4 Routers 是 IPv4 Node 構成，因此 6to4 Routers 處理流量全部源自於 IPv4 node 然而現今並沒有任何途徑對 6to4 Routers 上驗證對 IPv4 Node 所接收的資料，因此 6to4 網路理論上仍存在下列攻擊的可能性：(1)Neighbor Discovery (ND) Messages 的攻擊 (2)對 6to4 Nodes 進行 IP Spoofing 攻擊 (3)對 6to4 Nodes 進行 Spoofed Traffic 攻擊 (4)本地 IPv4 廣播攻擊。

在我們過去的研究中[4]顯示 Tunnel Broker 機制下進行的 4to6 DDoS 攻擊中發現不具備 IPv6 網路能力的主機也能產生 IPv6-in-IPv4 封包透過 Tunnel Broker 的轉送對 IPv6 網路中的電腦造成攻擊。此外在封包的資訊中顯示，IP Header 來源的 IPv4 位址欄位為 Victim 所連線的 Tunnel Broker Server 之 IPv4 位址，而來源的 IPv6 位址欄位則是亂數產生的 IPv6 位址。此外對目標進行 ICMPv6 Flood 攻擊時對 Tunnel Broker 轉換機制採取 IP Spoofing 的方式在檢查封包欄位異常部分，我們分析出 ICMPv6 Flood 攻擊封包中的 Type 欄位值為 128（ICMPv6 Echo Request），此時 Code 欄位應為 0，但攻擊封包的 Code 欄位值卻為 128，而其 ID 欄位始終為零。而無線上 Tunnel Broker 機制則為現階段我們所研究的內容之一。

隨著無線網路設備的普及，無線網路已迅速深入家庭及各級企業間，然而，在廣泛且大量的應用下，無線網路的安全性議題儼然成為當前重要課題。隨著 IPv6 時代的到來，IPv6 Home Network 裡無線網路的應用將更為廣泛，也因此，在無線 IPv6 網路的安全性更是需要被重視。一般在有線 IPv4 所具有的風險，在無線網路上依然存在著，甚至擁

有更多的風險，如無線網路上具有 WEP 加密、Rogue AP 等更多的問題。無線 IPv6 網路整合了 IPv6 網路所具有的優點，擁有較高的安全性，即使新一代 IPv6 網路具有較高的安全性，但無線 IPv6 網路上仍然是存在著安全性問題。因此本文特別針對無線 IPv6 的 DDoS 攻擊進行安全性研究。

3. DDoS Attack

「分散式阻斷服務攻擊」（Distributed Denial of Service, DDoS）是當前網際網路相當嚴重的安全問題。2002 年美國國防部先進研究計劃機構(DARPA)研究就指出[14]：DDoS 攻擊主要對攻擊目標採以發送大量的網路封包導致攻擊目標網路頻寬擁塞，或藉由大量的服務請求，使伺服器超出原有能服務的上限，進而造成耗損系統資源。也可針對 IPv4 網路上層通訊協定安全問題設計有缺陷的應用程式導致作業系統或硬體裝置在處理時發生不正常的情況，以及藉由緩慢的攻擊方式，進而導致系統或硬體的運作能力降低及有規劃性的操控路由表，導致網路流量不正常的被引導到其他網路或攻擊 DNS Server 讓網域名稱對應到錯誤的 IP 位址。

DDoS攻擊可依照利用網路協定弱點[9]分為以下幾種攻擊模式：(a)Flood Attack，一般是指攻擊者發送大量的網路封包去消耗特定受害者的網路頻寬，使得受害者的網路頻寬耗盡和系統癱瘓。這些攻擊常見的有UDP Flood攻擊和ICMP Flood攻擊。(b)Amplification Attack，利用ICMP協定的特質來做攻擊，並將目標指向Broadcast Address。(c)Protocol Exploit Attacks，針對TCP/IP Three-way handshake的特性進行攻擊，採用發出大量的SYN請求，並假造錯誤或不存在的來源位址，因而導致伺服端仍需等待timeout將該SYN請求結束，以及仍需處理接續大量的SYN請求，進而造成無法提供正常連線服務。(d)Malformed Packet Attack，主要利用異常的封包，以對受害者造成影響。其異常封包的攻擊又可分為兩大類：IP Address Attack和IP Packet options Attack。

近年來，新型結合蠕蟲的DDoS攻擊大量出現，如Code Red、Nimda、SQL Slammer等。Nimda造成全球大量的電腦遭受感染，數以萬計的郵件伺服器收到病毒郵件，讓伺服器的性能嚴重下降或是癱瘓，而影響整個網路的正常運作。Code Red為利用IIS的漏洞入侵系統並自我繁殖、傳播，形成攻擊。SQL Slammer蠕蟲則透過微軟SQL 2000的系統漏洞快速蔓延全世界，當SQL Slammer入侵有漏洞的系統後，便開始在網路上尋找其他有漏洞的主機，並與該主機建立連線，產生一傳十、十傳百的感染效應，形成分散式阻斷服務攻擊(DDOS)而癱瘓整個網路。

本文所關注的焦點在於 4to6 DDoS 攻擊。4to6 DDoS 攻擊是針對 IPv6 上的主機進行攻擊，攻擊者只要發佈攻擊的控制訊息，當 slave 端接收到，就會針對目標的 IPv6 主機進行攻擊。4to6 DDoS 攻擊最大的特色就是攻擊端與 slave 皆可不必支援 IPv6，只要擁有公開的 IPv4 位址就可在 IPv4 的網路上攻擊 IPv6 的主機，而 4to6 DDoS 攻擊主要就是透過 IPv4 與 IPv6 所建立的通道進行攻擊。

據我們所知，目前尚無詳細記載無線 IPv6 網路上 DDoS 攻擊的分析與偵測文件，因此，我們首先進行無線 IPv6 上的 DDoS 測試與分析，發現無線 IPv6 上的 DDoS 的攻擊仍然是存在著。

4. Detection and Prevention technology

為了分析與實測無線 IPv6 網路上的安全性，我們自行開發了 W6SGW(Wireless IPv6-enabling Security Gateway)。W6SGW 的架構如圖 1，主要由 Wireless IPv6、6IPS、Web-Based Management 3 個模組所組成。Wireless IPv6 使用 hostap 建置 Wireless IPv6 Access Point 功能，並透過 RADVD 發送位址，6IPS 是 Signature-based 為基礎的 IPS，它運用 Misuse Detection 技術來偵測網路攻擊，Web-Based Management 主要是利用 Tomcat 來建置與管理。

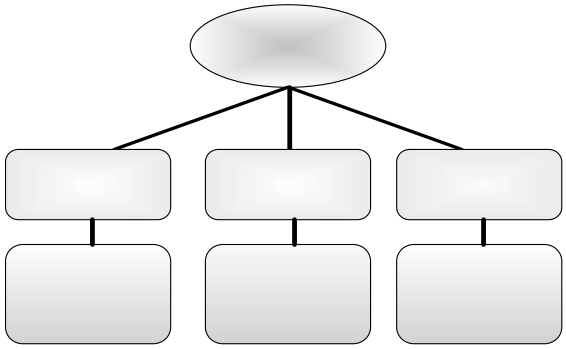

圖 1 W6SGW 架構

4.1 Detection technology

偵測技術方面我們結合了過去的開發經驗[5]，主要採用 Signature-Based Detection（又稱 Misuse Detection），其技術是由觀察已知事件並識別其誤用行為(Misuse Behavior)之後，再設計成可具體偵測其攻擊特徵的規則。Signature-Based Detection 主要以 byte-sequences 方式設計出唯一攻擊特徵，以及結合演算法設計相似特徵方法，最後在撰寫成攻擊模式資料庫。其最大缺點在於如果現行攻擊行為不存在於攻擊模式資料中，將無法偵測此行為，因此必須經常更新攻擊模式資料庫。

在針對 4to6 DDoS 的攻擊特徵分析上，Signature-Based 技術中常用的特徵規則(rules)已經不敷需求，因此我們採用最小計數原則(Minimum Counting Principles)並將其結合特徵規則撰寫成 Plugin。

其主要演算法如下：

```
global verdict_flag, rules_db
```

```
4to6DDoS(packet) {
   46DDoS_flag←0
   time_interval←120
   max_session←20

   signatures←get all s_col from rules_db where
    rules_name equal “4to6DDoS”
   for each packet.column: mapping in signatures
      if packet.column equal signatures.s_col
         46DDoS_flag←1

   construct_session_stat(packet, time_interval,
    max_session, 46DDoS_flag)

   if 46DDoS_flag = 2
      verdict_flag←serious
}
```

4to6DDoS Plugin 先從特徵資料庫的特徵取出後一一比對，更進一步建立以樹狀 Link-List 為基礎的連線狀態(session status)表，並在預先定的時間間隔(time interval)中計算出是否已超出預定的連線計數，如果兩者狀況皆成立，我們就將此連線的封包標記為 4to6 DDoS 的嚴重性攻擊封包。

4.2 Prevention technology

IPS(Intrusion Prevention System)依其運作模式可分為 In-line Mode 與 Tap Mode。In-line Mode 意指將 IPS 設置於網路通道上，所有網路上的流量都必須透過 IPS 轉發，Tap Mode 則是全雙工的監控網路上各方向的流量，可進行迂迴回應的動作。

IPS 的回應機制是屬於入侵回應系統(Intrusion Response System, IRS)中的一部份，入侵回應系統是一套機制完善的 IDS 警報處理系統。一般而言，IRS 本身並未進行入侵偵測的工作，而是基於 IDS 運作：IDS 送出警報至 IRS 之後，系統再針對不同的警報進行相對應的處理動作。IRS 依反應方式來分類，可將其分為 Notification Systems、Automatic Response Systems 與 Manual Response Systems 三種類型，以下整理表 1 來說明各種類型的 IRS。

表 1 – IRS 類型

Notification Systems	本質上與一般 IDS 的回應方式相同，主要是產生報告和警訊，但此系統包含更多的通報方式，例如發送 E-Mail、SMS 等，之後再由管理者作後續的處理動作。
Automatic Response Systems	此系統發展上傾向於取代管理者位置，原先須要依靠人員來手動進行的阻擋工作都由此系統自動的進行，IPS 便是屬於此類型的反應系統。
Manual Response Systems	與 Notification Systems 的回應方式雷同，差異在於 Manual Response Systems 會在發出警報之外產生幾項處理方式供管理者參考利用，不過最後依然要由人員手動將攻擊阻斷。

在我們實作的 IPS 整體架構如圖 2 所示，共分成五個模組與三個資料庫。實作上是採取模組化的方式進行，這方式不但可為以後提供更高的擴充性，也利於實作時的除錯之便利。

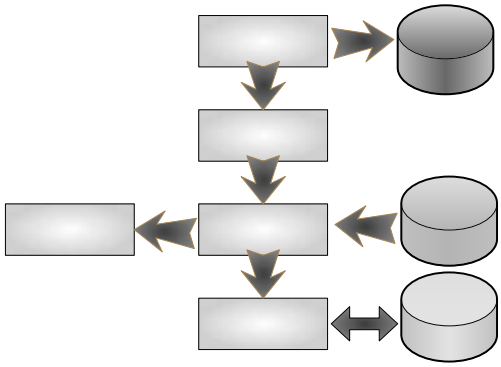

圖 2 IPS 模型

其中 Data Collector 模組主要功能為透過網路卡監聽所有網路流量，並擷取 IPv6 網路封包。Data Preprocessor 模組在接收到 Data Collector 模組轉送來的封包後，將得到的資訊儲存於標準化的格式中以利偵測的進行。 Intrusion Engine 模組會先將 Rules Database 中的規則讀出，接著持續的偵測 Data Preprocessor 模組所產出標準結構的封包資訊進行比對，若比對時與規則庫內描述的特徵一致時，便會對 Monitor & Alert Module 模組送出預期警示命令所需要的資訊。Monitor 和 Alert Module 模組在 Intrusion Engine 模組傳送警示命令資訊時做出相對應的行為，例如將遭受入侵或攻擊的相關資訊記錄或發出警報，此外也提供管理者可以監控正常流量與察看異常記錄。Event Database 存放著 Data Collector 模組解析過後的網路封包資訊。Rules Database 用來存放描述攻擊或入侵特徵的規則，規則將以通用的格式進行儲存。Message Database 主要存放著 Intrusion Engine 模組所偵測出的事件，經由 Monitor & Alert Module 模組觸發(Trigger)後所記錄，在管理者需要監控時，經由 Monitor & Alert Module 模組讀取與分析成格式化報表。

IDS 與 IPS 主要的差別在於 Response Module 部分。Response Module 主要是在接受到來自於 Intrusion Engine 的命令訊息，會做出對應的阻斷攻擊行為。

我們實作的演算法如下：

```
global verdict_flag, type_db

receive raw_packet and put in packet_queue
packet←new packet
packet.type←get type from type_db using
```

```
raw_packet.header as key
pass decode(raw_packet, packet)
pass detection(packet, verdict_flag)
switch(verdict_flag)
 case 0:
        packet.severity_level←normal
        forward(packet)
 case 1:
        packet.severity_level←warning
        forward(packet)
 case 2:
        packet.severity_level←serious
        drop(packet)
 default:
        packet.severity_level←unknown
        forward(packet)
next packet
```

由於 IPS 運作於 in-line 模式，因此我們必須先將接收的封包存放於佇列(Queue)中，在經過繁雜的解碼(Decode)與偵測(Detection)處理後，我們採以階層式等級(Hierarchical level)來區分其嚴重性及回應處理，例如偵測出並無存在任何攻擊的封包則將其標記為 Normal，並且將其轉送(Forward)；若偵測出 Port Scan 這類嘗試性並且不會直接造成傷害的攻擊，則將封包標記為警告性質，也將其繼續轉送；若偵測出 4to6 DDoS 這類嚴重性的攻擊封包，則除了發送警訊之外也將其封包丟棄(Drop)。

5. Scenario-based Testing of 4to6 DDoS attacks with W6SGW

建構完成 W6SGW 後，為了進行本次無線網路上 4to6 DDoS 攻擊的分析，我們已經先進行攻擊模式之特徵分析，並且已將這些攻擊模式的特徵寫入 W6SGW 規則庫，接著我們部署一個具有無線 IPv6 網路的實驗環境，並利用 W6SGW 及 Multimedia Server 進行以串流媒體為主的 Scenario-Based Testing，來證明 W6SGW 之有效性。

我們的測試場景如圖 3 所示，在此環境中我們建置了一個 Wireless IPv6 Home Network 的測試環境，其內部利用 Windows Server 2003 架設 IPv6 多媒體伺服器。我們利用 MN1 作為 Media Server 的 Client 端且透過 W6SGW 來觀看 Media Server 上的影像與聲音串流。在攻擊實作方面則由 Attacker 控制 2 台具有 Dual Stack 網路機制（IPv6 / IPv4）的 Slave，以及一台僅有 IPv4 網路的 Slave 來對 Media Server 發動 ICMPv6 的 Flood 攻擊，藉此了解到 4to6 DDoS 攻擊是否會對 Media Server 運作產生影響，以及 W6SGW 是否有發揮應有的效益。

我們的攻擊實測是針對運作中的 Media Server 發動攻擊。首先我們先使用 MN1 觀看 Media Server 上的影像及聲音串流並記錄下正常觀看影音的流量。接著才進行 4to6 DDoS 攻擊：由 Attacker 控制對 Slave 送出攻擊控制訊息，當 Slave 收到攻擊訊息後開始對 Media Server 產生攻擊流量，此時我們在 MN1 上會明顯的感受到影音串流的跳格及中斷現象。

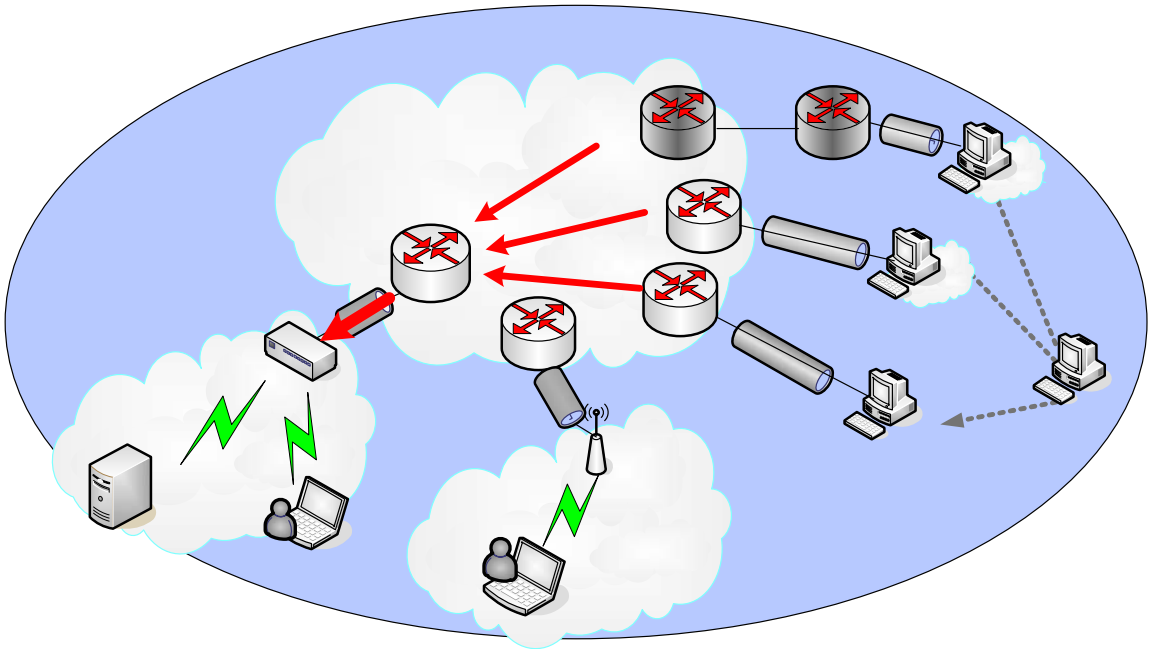

圖 3　W6SGW 攻擊測試環境圖

瞭解 4to6 DDoS 攻擊所造成的影響後，接著我們啟動 W6SGW 中的 IPS 功能，並透過 Web-Based 的監控畫面，如圖 4 所示，可以清楚的看到上方的監控視窗出現攻擊所產生的龐大連線數，且下方警

告訊息記錄也成功的紀錄下攻擊資訊。

圖 4　W6SGW 畫面

由圖 5 中可以清楚看到 W6SGW 之 IPS 功能啟動前與啟動後的攻擊流量比較。此次測試中我們分為 IPS 的啟動前與啟動後，且將兩次攻擊的封包大小與攻擊次數皆設成一樣的大小及次數，第一次測試沒有啟動 IPS，因此 Media Server 收到大量的攻擊封包，第二次測試時當攻擊流量約為第一次的一半時，便啟動 IPS，當 IPS 順利啟動時除了聽到硬體發出的警示聲外，Media Server 所遭受的攻擊封包也瞬間停止，IPS 順利的將攻擊封包阻擋下來。圖中實線方框則為攻擊的時間範圍。

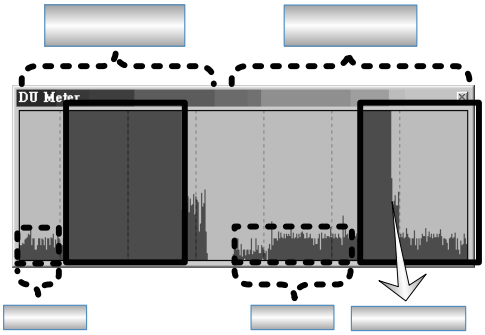

圖 5　IPS 啟動前後的攻擊流量比較

6. Conclusion

在轉換至 IPv6 環境的過渡時期，安全性的問題更是不容忽視的，唯有安全可靠且具便利性的 IPv6 環境才會被人們所廣為接受，W6SGW (Wireless IPv6-enabling Security Gateway)便是利於建置更具安全性及高可用性 IPv6 環境的工具。

本文主要針對無線 IPv6 進行安全性的分析，並指出在無線 IPv6 Tunnel Broker 機制下之 4to6 DDoS 攻擊仍然具有其威脅性。為了測試 W6SGW 的有效性，我們建置實驗場景來進行測試，結果顯示在無線網路的環境下，W6SGW 可正確地偵測並阻擋 4to6 DDoS 攻擊。

未來我們將更進一步對 Mobile IPv6 進行安全性分析。此外，我們目前的工作是關注於 Wireless IPv6 安全性分析與偵測技術上，下一階段我們將整合 W6SGW 模組至具有行動網路 M6SGW(Mobile IPv6-enabling Security Gateway)架構上，使其提供更完善的服務，以因應未來之需求。

Acknowledgement

本文感謝 NICI IPv6 R&D 分組計畫、電信國家型科技計畫 TWANST、教育部顧問室 94 年度「通訊科技人才培育先導型計畫」及 NSQC 實驗室程清智學弟支持，使相關實驗得以順利進行。

Reference

[1]. S. Deering and R. Hinden, Internet Protocol, Version 6(IPv6) Specification, RFC2460, Internet Engineering Task Force, December 1998.

[2]. A..Durand, P. Fasano, I.Guardini, D. Lento, ”IPv6 Tunnel Broker”,RFC 3053, January 2001.

[3]. B. Carpenter, K. Moore,” Connection of IPv6 Domains via IPv4 Clouds”, RFC 3056, February 2001.

[4]. Ching Feng Wang, Chi-Yuan Chen, Benjamin Tseng, Chi Sung Laih, "Detecting 4to6 DDoS Attacks on IPv6Network by Misuse Detection Technology," Proceedings of 2004 Taiwan Area Network Conference (TANet 2004), Taiwan, Oct. 2004.

[5]. Benjamin Tseng, Chi-Yuan Chen, Chi Sung Laih, "Design and Implementation of an IPv6-enabled Intrusion Detection System (6IDS)," Proceedings of 2004 International Computer Symposium (ICS 2004), Taiwan, Dec. 2004.

[6]. Templin, F., Gleeson, T., Talwar, M. and D. Thaler, "Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)", draft-ietf-ngtrans-isatap-22 (work in progress), May 2004.

[7]. Digital Living Network Alliance http://www.dlna.org

[8]. CERT CC. Denial of Service Attacks. http://www.cert.org/

[9]. Dave Ditrich, “Distributed Denial of Service (DDoS) attacks/tools resource page”, http://staff.washington.edu/dittrich/misc/DDoS/

[10]. P. Savola, C. Patel, Security Considerations for 6to4, RFC 3964, Network Working Group, December 2004.

[11]. P. Karn, P. Metzger, W. Simpson, The ESP DES-CBC Transform , RFC 1829, August 1995.

[12]. S. Kent, R. Atkinson, IP Authentication Header , RFC 2402 , November 1998.

[13]. S. Kent, R. Atkinson, IP Encapsulating Security Payload (ESP), RFC 2406, November 1998.

[14]. W.Hardaker, D.Kindred, R.Ostrenga, D.Sterne, R.Thomas. “Justification and Requirements for a National DDoS Defense Technology Evaluation Facility”, 2002 July.