Agent-Oriented Intelligent IPv6 Network Security Operation Center

Pei-Hsuan Huang * Cheng-Ying Lin ** Ching-Feng Wang * Benjamin Tseng ******

Department of Information Science, Hsing-Kuo University of Management*
Department of Information and Learning Technology, National University of Tainan **
Department of Engineering Science, National Cheng Kung University***
Department of Information Engineering, Kun Shan University****

hps1104@yahoo.com.tw
{bbaadd.bbaadd, smile.cf }@msa.hinet.net
drbt@mail2000.com.tw

摘要

現存IPv4網路存在有許多問題，如位址不足，安全性威脅等。為此新一代的IPv6網路協定在發展之初已提供許多的解決方案，但IPv6在實際的部署與實作上仍存在著其不足之處，特別是安全性問題。本文延續過去所進行的IPv6 IDS/IPS於大型IPv6網路上的安全性研究，並關注於現階段所出現之IPv6安全機制，無法提供大型IPv6網路或跨區域網路有效的解決方案，因此，我們特別設計並實作出”以軟體代理人為導向之智慧型IPv6安全監控中心A6NSOC(Agent-Oriented Intelligent IPv6 Network Security Operation Center)，整合Alert Filtering與Alert Correlation技術，以提供未來IPv6跨區域系統或大型網路所需有效率之安全管理方案。最後，我們並規劃Scenario-Based Testing來驗證A6NSOC，實驗結果證明A6NSOC確實能夠針對IPv6網路上不同程度之攻擊，有效進行警報嚴重性的區別與處理。

關鍵詞： A6NSOC(Agent-Oriented IPv6 Network Security Operation Center)、Alert Filtering、Alert Correlation。

1. Introduction

IPv4是當前網際網路所使用的主要網路協定，在早期主要作為提供相關學術團體與機構使用，因此在設計上並沒有考慮安全性問題，且規格的制定也欠缺完整性及周密性，隨著資訊科技的變化與需求增長，許多問題也跟著衍生而出。另外在Internet的快速發展的同時，Home Network的概念也開始出現，各式的資訊家電設備、手機、PDA 等行動上網設備的普及與所需的IP位址需求大幅成長下，加速現今IPv4位址的耗盡，據估計IPv4將於近幾年內耗盡。為了解決IPv4網路所出現的種種問題，新一世代的IPv6網路協定制訂之初便以2的128次方的位址空間克服了IPv4位址不足的問題，更以可擴展性、高度的移動性和更為具體之安全性，擴大了可應用的層面，滿足了未來資訊網路日趨發展的的需求。

在資訊科技快速發展的今天，資安的問題仍然伴隨著資訊化的迅速發展下日趨嚴重，其中國家的國防或經濟等重要資料也因網路的應用下使得機密資訊遭竊取的案例層出不窮。例如：在2000年初，Yahoo、Amazon、CNN、eBay 遭到分散式阻斷服務(Distributed Denial of Service：DDoS)的攻擊、2005年對岸的駭客也透過木馬程式大舉入侵我國的軍方單位與民間企業。這些攻擊皆造成了政府與企業龐大的損失。因此，近來人們對網路安全性的重視也逐漸提升，許多的安全性設備陸續的被提出，但目前多數的安全性設備大多屬於單一地區性或小型網路所使用之方法，面對大型或跨區域之攻擊，則無法提供有效的解決方案。對此，無論政府機關或企業用戶，都需建立一個全面性的資安事件整合機制，其作法為透過一個安全監控中心來監控部署於網路中的Sensor，以了解網路最新情況。

為了解決現今網路的限制，邁向IPv6網路協定將是必然的趨勢。新一代網際網路意味著更多的應用、更快的速度和更大的規模。但是，隨著網路應用的增加、速度的加快和規模的變大，必須面對更多的安全風險。IPv6設計之初，已擁有龐大的位址空間，儘管如此龐大的位址空間間接提升了位址掃瞄的難度，並加上強制性要求實現IPSec。由IPv6的眾多特性我們認為，新一代網際網路應更為安全，但是IPSec由於密鑰管理問題仍然難以廣泛部署和實施，且大部份的攻擊發生處主要是在應用層而不是網路層，因此IPv6網路仍然面臨許多安全問題。

就我們過去研究指出[13][14]，IPv6 現階段安全性問題最大的部份在於 IPv4 /IPv6 間的轉換機制。由於要從 IPv4 網路完全轉移到 IPv6 網路現仍有許多技術更換的問題尚待解決，且需在對現有基礎設施升級和需要龐大資金投入基礎建設。為了讓 IPv6 與 IPv4 環境共存，IPv6 網路目前仍需透過一些轉換機制與 IPv4 網路共存。目前這些不同轉換機制在架構上缺乏完整的安全性考量，以至於仍有許多來自上層通訊協定的安全性威脅等問題存在，導致許多攻擊其實是透過 IPv4 攻擊 IPv6，進而影響 IPv6 網路上的主機。

近幾年IPv6的成長相當的快速,在轉換至IPv6環境的過渡時期，安全性問題能否克服，如此將直接影響到IPv6是否容易廣為人們所接受。面對IPv6上的攻擊威脅，我們過去也提出6IDS[3]、6IPS[14]和 W6SGW[13]等適用於 IPv6 網路安全之解決方案。在本文中，我們將以過去既有的研究與開發經驗下,提出以軟體代理人為基礎之IPv6安全監控中心以解決未來IPv6網路所需之必要安全管理監控。

本文的主要目地是研究 IPv6 網路安全監控中心。本文其餘內容如下，第二節討論過去對於安全監控中心的研究以及技術發展；第三節說明智慧型IPv6網路安全監控中心的系統架構;第四節是IPv6網路安全監控中心所使用的智慧型技術；第五節則是A6NSOC的實作,同時並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. Background and Related work

近年來由於 IPv4 網路所存在的許多問題，進而使得 IPv6 網路相關之研究逐漸受到專家學者的關注，期望能克服IPv4網路的缺陷與問題。但是相關學者多年來的研究指出，IPv6也仍存在著安全性問題[14]。過去的研究中[14]顯示，透過 Tunnel Broker 機制與 IPv6 網路進行連結仍然可能會遭受DDoS攻擊，其中所進行的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。另外，在過去的研究中也指出無線IPv6 網路上仍然存在著其威脅[13]。在其他轉換機制上,P.Savola與C.Patel[9]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網路理論上仍存在著由IP Spoofing所導致的攻擊。

另外，在IPv4網路中，由於安全性問題日益嚴重，以及安全防護設備受限於無法滿足大型網路防護的實際需求。對此，Security Operation Center的相關技術也陸續提出。在現今Security Operation Center用於IPv4網路上，目前已有相關文獻有記載一些解決方案。但就我們所知，目前尚無相關文獻記載適用於IPv6網路之Security Operation Center。有鑑於此，我們進行IPv6 Security Operation Center之研究，並透過Agent-oriented之設計整合Alert Correlation、Alert Filtering之智慧型技術來加強安全管理監控之處理流程。

隨著網路技術的成熟，由於Agent[8][15]技術具有許多優點如其代理性(Delegation)、自主性(Autonomy)、機動性(Mobility)、溝通技術(Communication)及等特性，因此，Agent技術廣範應用於網路應用上以及許多系統也已Agent-oriented的方向進行設計，同時也在許多系統上獲得不錯的成效。Agent依其移動（Mobility），又可分為固定代理人（Stationary Agent）與行動代理人（Mobile Agent）。而目前也有許多Agent系統工具，如：MS Agent、IBM Aglet及Voyage[15]。MS Agent為一ActiveX控制元件，主要應用於使用者介面上。IBM Aglet為一輕量級的代理人(Light-weight Agent)系統工具。Voyager是由Recursion公司所開發，為一付費軟體，純使用Java環境的分散式計算平台，可用於迅速開發其高性能之分散式應用程式。

Alert Correlation技術中，A. Valdes和K. Skinner兩位著名學者提出的Probabilistic Alert Correlation[2]，此方法利用警訊內容來做警訊屬性的關聯，對每一個屬性都給予一個適當的相似度函數。Peng Ning等學者[10]，整理完成用來描述攻擊行為之必要條件(prerequisite)及事後結果(consequence)的規則，並提出Hyper-Alert Type的概念,實作離線警訊關聯器（off-line Alert correlator）。Frédéric Cuppens提出CRIM架構[9]，此架構主要由五大模型,此五大模型包含警報管理功能(Alert base management function)、警報叢集(Alert Clustering)、警報合併(Alert Merging)、警報關連(Alert Correlation)、目的確認(Intention Recognition)。另外,SIP Lab提出一個TRINETR架構,此架構為一入侵警訊管理系統,主要有三大元件，警報聚集(Alert Aggregation)、警報評估知識庫(Knowledge-based Alert Evaluation)、警報關連(Alert Correlation)[12]。Sunu Mathew, Chintan Shah, Shambhu Upadhyaya[11]等人透過分析Alert的資料來發現相關的攻擊，此篇論文中並提出了以活動中的Alert串流為基礎來建構出圖形化的攻擊場景，並說明開發一套攻擊場景的架構，使得更容易刪除Alert以及更可靠的計算、推估其場景。

使用Alert Filtering之技術有許多種方法，其中一種方法是建立該網路拓撲之Profile。並利用工具來建立Profile,接著與IDS所產生之Alert進行比對，並將誤報之Alert加以刪除。Profile的建立方式可透過Active Fingerprinting、Passive Fingerprinting兩種方式來完成，或者依照應用的類型所分成的OS Fingerprinting、Application Fingerprinting及Web Fingerprinting技術來建立Profile。另一種Alert Filtering之技術為透過Priority來進行Alert的Filter，使用Priority首先會給予每條規則一個優先級別，依照其及別將低等級之Alert刪除。

就上述的方法技術與我們的瞭解，目前尚無相關文獻與系統記載IPv6網路之Security Operation Center。因此本文提出適用於IPv6網路安全防護與提升後端安全管理人員效率之新的解決方案A6NSOC。

3. Agent-Oriented Intelligent IPv6 Security Operation Center

具我們所知，A6NSOC 是第一個可部署於大型 IPv6 網路的安全監控中心。本文主要是以 Agent[8][15]導向為基礎進行系統之設計，因代理人(Agent)具有代理性(Delegation)、自主性(Autonomy)、機動性(Mobility)、溝通技術(Communication)等優點，故已被廣泛運用到網路應用上。透過代理人(Agent)使其能依照使用者的指示和想法來運作，甚至代表使用者來處理事件，也能主動與其所處的執行環境相互溝通，進而完成使用者委派的任務，因此本系統以 Agent 導向為基礎進行系統的開發。

由於入侵偵測系統運作的同時會蒐集到許多的 Alert，這些 Alert 中並不是全部皆符合我們的系統環境或者為誤報，此時我們就必須把此 Alert 加以排除。對安全防護中心而言，入侵偵測系統必須將所蒐集到的龐大 Alert 傳回中心，若全部傳回至中心，則會造成中心過多的負擔，因此我們的作法為先將 Alert 加以過濾、排除，把正確的 Alert 傳回至中心，以供後續動作。對此本系統採用 Intelligent Agents[7]技術進行開發，整合 Alert Correlation 與 Alert Filtering 機制，以達到降低不必要之 Alert，減輕管理人員之負擔。

3.1 A6NSOC系統架構

A6NSOC 主要分為 IPv6 Security Center 與 Sensor兩大部分，以下為此系統之架構。此系統中我們也採以階層式架構進行Alert Correlation。在不同的區域中，我們各別部署了幾台Sensor，這些Sensor分別可對所屬之區域網路進行安全性偵測，並透過Agent之技術，自動將偵測到之訊息經由正規化、Local Correlation與Filtering後，快速傳送回IPv6 Security Center。而在IPv6 Security Center端部署Aglet Server，用來接收Sensor傳送之訊息，並儲存至資料庫，進行後續Global Correlation之處理。

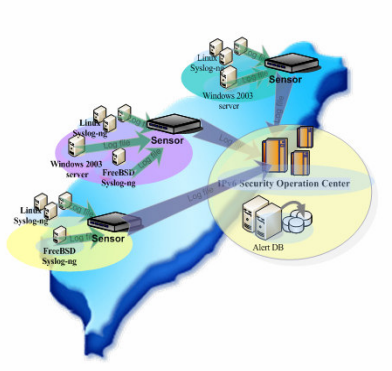

圖1 A6NSOC系統架構圖

3.1.1 IPv6 Security Center

IPv6 Security Center所使用之系統元件皆擁有跨平台之功能，因此系統可建置於Unix或者是Windows系統上，我們將IPv6 Security Center建構在Windows系統上，使用Tomcat建置Web Container，透過JSP程式語言進行網頁存取，提供管理者監控畫面，讓管理者能夠迅速瞭解不同區域之網路狀態，以進行後續之處理。此外，IPv6 Security Center還提供了Filtering和Global Correlation處理機制，並透過網頁方式來表達其處理過的資訊，讓管理者能夠更輕易的透過網際網路以Web模式進行系統控管和監控。

3.1.2 Sensor

Sensor部分，我們主要是延續先前所開發之6IDS元件[3]，增強改以Agent導向之設計進行系統架構上之修正與增加新功能，如IPv6 Access Point，Alert正規化，並提供了Local Correlation的處理機制，對於警訊做相關的處理，以便於能快速將嚴重警訊傳回IPv6 Security Center。

Sensor中主要系統如下圖所示，分為六大模組，詳細說明如下，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。

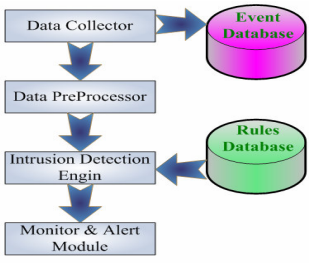

圖 2 6IDS 系統模組

3.2 Alert Correlation 技術

警報的高錯誤比率是至今入侵偵測技術仍需

克服的關鍵問題。由於一般的 IDS 都是根據單一事件進行分析，因此一個入侵行為下便會造成許多警報的產生。為了處理這些問題，許多研究人員提出以警報的關連性進行處理的觀念。從警報的關連性中推測入侵事件是否關連，若入侵的事件被連結，則此事件應具有相關性，若非則將此警報隔離。本文現階段的作法為利用 Alert Correlation 技術將 Alert 進行刪減，讓原本數筆相同之 Alert 變成單筆，並送回 Security Center。其演算法如下:

```
While loop{
if(alert∈Port Scan Attack) {
    if(count == 0) {
          cor_alert ← alert.allinfo
          SourceIP ← alert.SourceIP;
          ack_time ← alert_time;
          distIP ← alert.disIP;
          count++; }
       else{
          tmpip ← alert.SourceIP;
          tmp_ time ← alert_ time;
          tmpdistIP ← alert.distIP
          if(SourceIP,tmpip, ack_ time, tmp_ time
And distIP,tmpdistIP are equal){
                  count++;
                  detect alert;
                  continue; }
          else{
             output cor_alert;
             cor_alert ← alert.allinfo;
             SourceIP ← alert.tmpip;
             ack_ time ← alert_ time;
             distIP ← alert.distIP;}
          }
       }
   }
}
```

3.3 Alert Filtering 技術

若是直接將各 Sensor 所蒐集的警報事件直接傳回到 Security Center，將會有大量的 Alert 塞滿 Security Center 端的監控畫面，此時反而造成無從分析或仍需大量人力解析這些事件的意義，這些都不適合於大型安全監控中心的運作。因此在 A6NSOC 中，我們首先進行警報整合與過濾。這主要的警報整合工作如果在配合適當的過濾機制來分別處理不同嚴重性的警報，將最嚴重的警報事件迅速回傳到 Security Center，由 Security Center 立即進行後續的回報與入侵事件處理，而其他比較不嚴重的警報事件則可以視工作負載來進行回傳。要做到如此將不同事件進行優先權的設定，必須考量不同範圍的優先權的設定，我們主要利用優先權對 Alert 進行過濾。

本系統之優先權等級共分為五級。等級 1 為 INFORMATIONA，此為對 Sensor 有助益的資訊。等級 2 為 SUSPICIOUS，代表 Sensor 所監控到的資安訊息，但未被定義成威脅事件。等級 3 為 THREAT，表示可能會成為具威脅性的事件。等級 4 為 CRITICAL，已造成的威脅事件，並於 Security Center 產生 ticket。等級 5 為 LARGE SCALE Attack，Security Center 取得兩個 Sensor 以上的資安訊息、事件。在我們的測試中，一般都只見到 1 至 4 級的優先權。第一階段 Sensor 所處理的優先權設定只有 1 至 4 級的優先權，而第二階段 Security Center 端優先權的設定則主要是針對大型網路攻擊事件所進行的優先權，由於大型網路攻擊事件會跨越大範圍的攻擊，因此在部署的其他 Sensor 也應該會遭受攻擊。

4. Implementation and Testing

4.1 Implementation

本系統的開發環境主要分為 IPv6 Security Center 和 Sensor 兩大部分。其中所使用的環境與軟體如下：

表 1 系統開發環境

IPv6 Security Center	
OS	Windows XP SP2
JVM	J2SDK 1.4.2
Database	MySQL 5.0.22
Web container	Apache Tomcat 5.5
Sensor	
OS	Linux Redhat(kernel 2.9)
JVM	J2SDK 1.4.2
6IDS	C Language

本系統以 Java 做為我們系統應用及分散式程式架構開發之基礎語言採用 Java 最主要目的為具有跨平台"Write Once，Run everywhere"之特性，使得未來 IPv6 安全監控中心系統能廣泛應用在各種異質的環境平台上。我們使用的 Agent 環境是 IBM Aglet[1][15]，Aglet 為建立在 Java 平台上提供開放原始碼(Open Source)的代理人系統，且具平台獨立性(Platform Independence)的優點，在其運行之主機上具備標準的 Java 虛擬機器，Aglet 平台即可不必相依於所執行的主機直接起動，而 Aglet 更可將 Java 所提供的動態類別載入(Dynamic Class Loading)

機制於 Aglet 平台中運作和自動將設計好的 Agent 程式載入執行。此外，Aglet 也支援其多執行緒機制，因此在 Aglet 平台上所執行的代理人(Agent)程式，皆可各自在其分配的執行緒上同時執行。

在 IPv6 Security Center 中，我們現階段將系統建置在 Windows 平台上，以 While loop 方式建立一事件監聽模組，當事件觸發後，藉由 Aglet 動態類別載入 (Dynamic Class Loading)，將其 Communication 模組載入執行。Communication 模組負責處理 Sensor 端傳送之警訊，處理完畢後，Communication 模組會透過 Aglet 所提供之 dispose() 進行銷毀，而警訊則透過資料庫模組寫入資料庫，再交由智慧型模組進行 Filtering 和 Global Correlation 之處理，最後再依其警訊之嚴重性，透過網頁的方式，顯示在管理者監控畫面中。

另外在 Sensor 中，我們以 Linux 平台延續先前的 6IDS[3]為開發基礎。Sensor 端同樣具有一事件監聽模組，判斷是否有警訊產生，一旦產生警訊，Aglet 便立即載入警訊處理模組，將警訊傳送至 IPv6 Security Center。同樣的，當警訊處理傳送完畢，此模組會經由 Aglet 之 dispose()功能將其銷毀。

4.2 Scenario-based Testing

為了測試 A6NSOC 的有效性，我們規劃了 Scenario-based Testing，並部屬了 4 種攻擊測試，以驗證我們系統的有效性。其攻擊測試說明如下：(1)一般情況下的流量：此測試中，我們在 Sensor 所保護的區域，建置 Web Server、FTP Server 等等一般使用者常用的伺服器，並進行存取，以及觀看正常流量。(2)Port Scan：我們利用 IPv6 網路上的主機對於 Sensor 內部之機器進行，Port Scan，並觀看 Sensor 與安全監控中心是否有所回應。(3)4to6 DDos Attack：我們利用一台攻擊者操控 3 台 Slave，其中兩台 Slave 透過 Tunnel Broker 機制連線至 IPv6 網路，另一台則為純 IPv4 之 Slave，透過操控這 3 台主機對 Sensor 所保護之 Server 進行 DDoS 攻擊，同時，我們也觀看 Sensor 與安全監控中心是否有所回應。(4)跨區域之 DDoS Attack：如同攻擊測試 3，我們同時對 2 個區域進行 DDoS Attack，察看 Sensor 與安全監控中心是否有所回應。

在下圖的測試場景中，進行Port Scan測試時，我們使用6to4轉換機制讓裝有NMAP的掃瞄端(Scanner)連上IPv6網路，面對使用Tunnel Broker機制的C Sensor發動掃瞄攻擊；在4to6 DDoS攻擊部分，其中Attacker控制兩台具有Dual Stack網路機制（IPv6/IPv4）的Slave，以及一台僅有IPv4網路的Slave，攻擊Location A中的A3 Server。實際的攻擊行為是由Attacker以4to6的DDoS攻擊對Slave發送攻擊指令，當Slave收到攻擊指令便立即透過假冒的Tunnel身份（設定於Tunnel兩端的Public IPv4位址）對Tunnel Broker Server送出大量IPv6目的端位址為A3的ICMP Flood攻擊封包，再經由Tunnel Broker轉換機制送到A3。跨區域之DDoS Attack，我們也增加了對Location B中的B1 Server進行DDoS Attack。進行上述攻擊之同時，我們會同時觀看IPv6 Security Center與Sensor之變化。

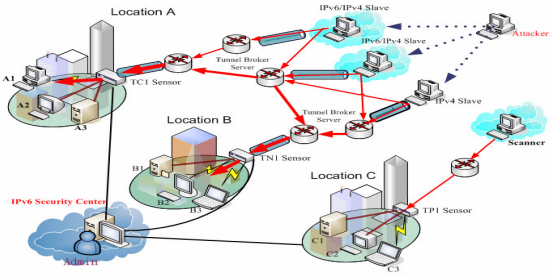

圖3 攻擊場景圖

測試結果說明如下：(1)一般情況下的流量：此結果我們所看到的訊息為 Sensor TC1 內部之 Server 為正常流量，安全監控中心並無警告或嚴重訊息。(2)Port Scan：我們以很快的速度在安全監控中心中獲得 TP1 Sensor 被攻擊之訊息。(3)4to6 DDos Attack：我們偵測到 Sensor TC1 中的 Server A3 瞬間產生大量的流量，並且於安全監控中心顯示出遭受 DDoS Attack。(4)跨區域之 DDoS Attack：我們於 Sensor TC1 中的 Server A3 與 Sensor TN1 中的 Server B1 皆偵測到大量的流量，並且於安全監控中心中顯示遭受攻擊。

以下為IPv6 Security Center之監控畫面，監控畫面首先顯示各Sensor之IPv6位址，接著顯示各Sensor之網路監控情形並顯示出Priority，透過Priority我們可得知這些封包訊息使否存在著威脅，如Priority為4則表示為DDoS Attack。此外，IPv6 Security Center還會對於所監控之Sensor進行攻擊比對，如在兩個區域皆出現DDoS Attack，則表示為跨區域之攻擊，優先權會自動加1，升級到Priority5，此時所代表的訊息危急，提醒管理者必須立即處理。接著會顯示Sensor所受到攻擊之訊息，說明Sensor發生事件的名稱，最底下之視窗，如果發生跨區域之DDoS Attack，則會顯示出遭到跨區域DDoS Attack之Sensor名稱。

具我們實驗結果可證實，本系統之IPv6安全監控中心確實能夠有效偵測出IPv6網路上之攻擊，並

將所偵測之結果，回傳至IPv6 Security Center，以避免不必要的損失。

圖4 A6NSOC之監控畫面

5. Conclusion

本系統所針對的就是新一世代IPv6網路上的安全性研究，並以Agent導向為基礎之設計理念所開發出來的。此系統之雛形除了可用於小型區域網路外，更延伸以大型或跨區域性的IPv6 Network安全性回報需求進行設計開發，同時適用於有線網路外，對於近年來熱門的無線網路，我們也針對IPv6 Wireless Network進行研究與探討，將其功能整合在此系統上。本系統主要整合Alert Filtering、Alert correlation技術開發Intelligent Agents，用以處理大量和排除不必要Alert，提供嚴重性高的Alert回送IPv6安全監控中心，以利管理者能夠有效的掌握各區之網路攻擊現況。

本系統現階段已完成初步雛型，下一階段期望將朝向增加以網路拓樸之Profile技術進行誤報Alert的刪除，提升系統過濾的能力。

Acknowledgement

本文特別感謝 NICI IPv6 R&D 分組計畫與 TWISC@NCKU(NSC 94-3114-P-006-001-Y) 的支持，使相關實驗得以順利進行。

參考文獻

[1] Aglet,http://www.trl.ibm.com/aglets/.

[2] A.Valdes, K. Skinner, “Probabilistic Alert Correlation”, RAID 2001

[3] 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.

[4] Ching Feng Wang, Chi-Yuan Chen, Benjamin Tseng, Chi Sung Laih, "Detecting 4to6 DDoS Attacks on IPv6Network by Misuse Detection Technology," TANET 2004(Taiwan Area Network Conference 2004), 10/2004

[5] Frédéric Cuppens, Alexandre Miège, “Alert Correlation in a CooperativeIntrusion Detection Framework ”, IEEE Symposium on Research in Security and Privacy2002 , 2002.

[6] Honeynet Project,http://project.honeynet.org.

[7] Joseph P. Bigus, Jennifer Bigus, Joe Bigus "Constructing Intelligent Agents Using Java: Professional Developer's Guide, 2nd Edition", Wiley,2001.

[8] M. Wooldridge, "Introduction to MultiAgent Systems", John Wiley&Sons,2002.

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

[10] Peng Ning, Douglas S. Reeves, Yun Cui, “Correlating Alerts Using Prerequisites of Intrusions”, Technical Report, TR-2001-13, North Carolina State University, Department of Computer Science, December 2001.

[11] Sunu Mathew, Chintan Shah, Shambhu J. Upadhyaya: An Alert Fusion Framework for Situation Awareness of Coordinated Multistage Attacks. Third IEEE International Workshop on Information Assurance IWIA 2005: 95-10

[12] Vijayanand Bharadwaj, Y. V. Ramana Reddy, Kankanahalli Srinivas, Sumitra Reddy, Sentil Selliah, Jinqiao Yu: Evaluating Adaptability in Frameworks that Support Morphing Collaboration Patterns. WETICE 2004: 186-191

[13] Zheng-Ying Lin, Yong-Ming Huang, Chi Yuan Chen, Benjamin Tseng, “Detection and Prevention of DDoS Attack over Wireless IPv6 Network”, TANET 2005(Taiwan Area Network Conference 2005), 10/2005.

[14] 曾龍,陳麒元,王慶豐,林政穎,陳柔伊,黃培軒,莊富傑,紀佳津, “IPv6 網路攻擊及防禦”,第十三屆三軍官校基礎學術研討會,05/2006

[15] 竇其仁,林志敏,林正敏, "網路代理人 Network Agents",知城數位科技股份有限公司,2006.