以 OpenFlow 交換器建構網路安全防禦系統之研究與實現

葉曉霈 [a]、蕭紋旭 [b]、陳景章 [a]、洪光耀 [a*]
國立中正大學通訊工程所 [a]
吳鳳科技大學應用數位媒體系 [b]

摘要 —本論文提出運用 OpenFlow 平台進行安全管理與防護，並提供一個整合型安全防護機制，保護使用者網路安全，防範外部入侵者，同時也監控內部使用者，形成安全網域，增加網路安全。網路安全防禦系統系統實現於 OpenFlow 平台上，系統包括 OpenFlow 交換器、控制器負責依決策結果進行防禦動作，並結合入侵偵測系統監測網路內部情況，且建立安全事件決策系統，對可疑事件進行分析與決策，保護使用者網路。

一、 前言

隨著電腦普及化的運用與網際網路的蓬勃發展，因此網際網路攻擊多變與範圍廣泛，如 2013 年 5 月發生的資安事件[1]台灣 Groupon 被駭，約 38 萬用戶帳密外洩；中國信託繳費中信網站外洩大量用戶個資；台、菲網路分散式阻斷攻擊；日本雅虎 2200 萬筆使用者 ID 遭到非法存取 。目前網路攻擊演變迅速，容易造成大量個資外洩與龐大的金錢損失，進而影響使用者使用服務的意願，因此網路安全和攻擊事件的分析與處理是相當重要的議題。而傳統的網路管理系統與現今的資訊安全監控中心同時整合許多不同的資源與資訊，但這兩種系統幾乎都是個別獨立運作，如何做有效的監測，如何從眾多的資訊中擷取有效的資訊，如何進一步處理、決策都是考驗。

OpenFlow 交換器與傳統交換器不同的是將控制層與資料層分開，而控制層由軟體負責網路管理，且可以在控制層開發應用程式並部署於控制器內，再藉由 OpenFlow 的安全傳輸通道連繫資料層的 OpenFlow 交換器，OpenFlow 交換器則專責於封包傳送，提升傳輸效率。部署 OpenFlow 能降低網路裝置複雜度並透過簡化網路管理達成工作自動化，亦可節省企業的營運成本。

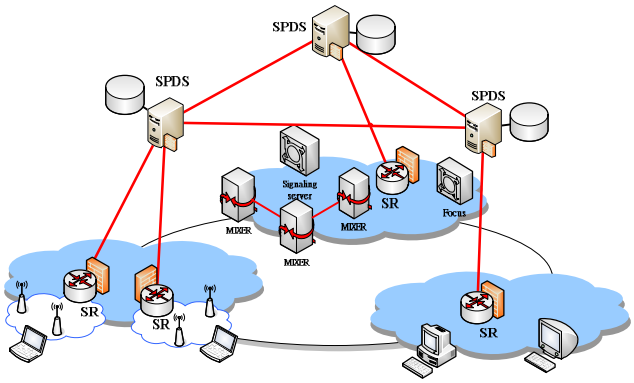
本論文提出運用 OpenFlow 平台進行安全管理與防護，並提供一個整合型安全防護機制，保護使用者網路安全，防範外部入侵者，同時也監控內部使用者，形成安全網域，增加網路安全。

本論文參考[2]所提出的系統架構根據應用的環境與服務之需求來設計修改系統。實現於 OpenFlow 平台上，OpenFlow 交換器、控制器負責依決策結果進行防禦動作，並結合入侵偵測系統監測網路內部情況，且建立安全事件決策系統，對可疑事件進行分析與決策，保護使用者網路安全。針對常見大規模的阻斷式服務(Denial of Service, DoS)網路攻擊做系統測試。

二、 相關研究

2.1 分散式防禦系統

在[2][3]提出由網路服務提供業者(ISP)提供的網路安全防禦服務，該網路安全防禦服務的系統建置於 ISP 原有的網路結構上，於 ISP 的核心網路中建置安全決策中心進行安全事件的政策決策，以及在網路邊境的路由器上建置防禦系統形成一個具有安全保護的網域稱為安全網域，透過各安全網域的防禦系統進行網域的網路監控與過濾威脅流量提供使用者網路安全防禦服務，在系統架構中部署決策系統(Security Policy Decision Server, 安全政策決策系統)作為政策決定之用，且與其他網域溝通進而達到區域聯防，而系統各網域的路由器，皆為部署安全路由器做為封包轉送、監控與過濾。其中安全政策決策系統政策決定的部分，主要是談論 Policy Management 安全政策之運作機制。

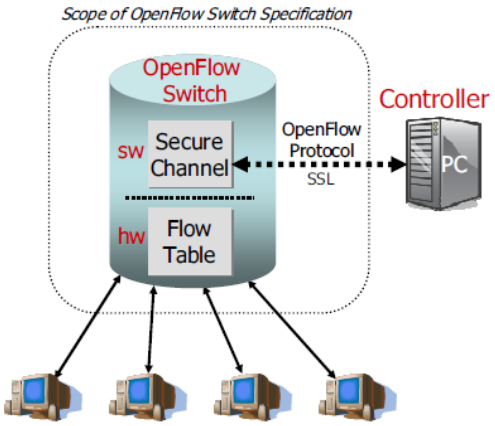


圖一: 分散式之防護對策裝置系統架構圖

2.2 Openflow 架構介紹

OpenFlow 網路架構，主要由OpenFlow 交換器與控制器〈Controller〉所組成，傳統第二層交換器 將控制層與資料層實作於交換器 之內，然而OpenFlow交換器則是將控制層與資料層分開。Openflow交換器[4]可以讓研究人員測試自己設計的協定或政策，在交換器中，利用 Flow Tables去新增或刪除Entry來管理整個網路，可以達到line-rate和支援多台電腦且可以做防火牆、NAT和狀態的蒐集。

Corresponding author:K.Y.Hong0815@gmail.com
DOI:10.6159/IJSE.2014.(4-2).92



圖二: Controller 透過 Secure Channel 連結 Openflow 交換器[4]

Controller 是一種網路的控制平台如 NOX、Floodlight、OVS controller，允許研究者自行撰寫相關之功能，讓網路管理和應用控制可以建立，使用者和網路管理者可以在Controller上對底下任何的交換器設定封包的流向。

OpenFlow 透過Controller去管理底下的每個電腦的封包傳遞，Stanford University[4]是利用NetFPGA當成Openflow交換器，將Flowtable做在硬體上，根據封包的不同可以快速查閱，圖二表示Controller透過安全通道去和每一台 Openflow 交換器作聯繫。Openflow 交換器網路環境三大要素：

(1) Flow Table：定義每個 Flow 的行為，來告知交換器如何去處理每一個 Flow 。

(2) Secure Channel ： 連接 交換器 與遠端控制的 Controller ，可以用來下達命令或是傳遞封包。

(3) Openflow Protocol：提供一個標準讓 Controller 和交換器互相溝通。

Openflow 交換器 處理封包流程如下：當封包進入到交換器時，會進行 Flowtable 的比對，不符合 Flowtable 時就會透過安全通道轉送給 Controller 進行處理，由 Controller 決定好封包的動作，會新增 Flowtable 連同封包回傳給交換器，交換器會依造新增的 Flowtable 做處理。

2.3 運用 OpenFlow 建構安全機制

討論OpenFlow 交換器應用於網路安全管理，針對殭屍網路，[6][7]使用OpenFlow 交換器分析偵測殭屍網路，藉由OpenFlow交換器平台具有的快速導向功能及虛擬網路，實際分析電腦感染後行為，透過OpenFlow交換器通知感染的使用者解毒，阻斷其與駭客之間的聯繫；輕型檢測分散式阻斷攻擊[8]OpenFlow Controller監測交換器，在時間間隔內收集進入的Flow Entry提取現有的特徵，Controller 加入Self Organizing Maps (SOM)邏輯法進行分類、判斷是否為攻擊，達到降低錯誤率自動化檢測；[9]則是提出分散式阻斷攻擊攻擊防禦在OpenFlow 交換器上實現。 OpenFlow的交換機可以監控流量通過批量計數和檢測分散式阻斷攻擊攻擊，基於自我維護機制，DDoS攻擊防禦可以自動化運作；以OpenFlow網路為基礎設計與實現Procera [10] ，Procera為事件驅動網路控制架構基於functional reactive programming (FRP)，營運商可以用Procera表達高等級的策略，且會將策略轉換成轉向的規則，並將其部署在校園，校園的網路是由OpenFlow組成的，得到的成效Procera和OpenFlow可以大大減少網絡配置和管理的工作量，並輕鬆引入額外的功能到網絡。可以得知與傳統技術不同，OpenFlow可快速導向封包、提供虛擬網路、分層可程式化可靈活與安全設備作搭配。

表一:傳統技術與OpenFlow技術比較

	Network Device	OpenFlow
優點	現有成熟設備與協定，網路設備擁有高性能	快速導向封包、成本低、自動化
缺點	1.路由表越來越複雜 2.網管軟體彼此之間難以相容 3.必須針對每臺交換器或路由器，逐一登入命令執行介面	1.控制器必須要去承受資料流的壓力，較容易造成效能瓶頸 2.現階段要開發應用程式的門檻較高

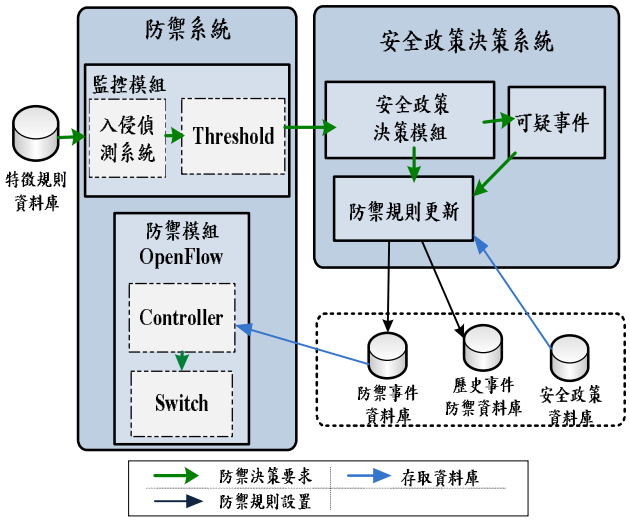
三、 系統設計和架構

3.1 系統環境

本論文的系統架構是基於[2][3]論文中所提出的架構，運用 OpenFlow 平台實現出來，並測試安全機制的完整度。本系統整體環境主要是建立群組分散式的防務系統，各個網域的出入口上，設置防禦系統進行各網域網路的監控與防禦，而被監控與防禦的網域稱為安全網域(Security Domain)，此外藉由多個安全網域的監控系統監控各網域，進而達成分散式收集網路攻擊資訊在各網域中部署一台安全政策決策系統作為政策決策之用，而 OpenFlow Controller 會依據決策對其負責之 OpenFlow 交換器進行控制。

3.2 系統架構及設計

圖三為網路安全管理系統的架構圖主要分為個實體元件，分別是防禦系統與安全政策決策系統，防禦系統主要進行前端的安全管理，由Controller 和Switch對入口處進行封包過濾與管控，而入侵偵測系統在安全網域內部進行監控與蒐集、規則比對，將蒐集到的封包傳給後端的安全政策決策系統，更進一步的分析驗證其攻擊性與該採取的政策，以下針對這兩個主要元件內部描述說明。



圖三:網路安全防禦系統之精簡架構圖

防禦系統，前端設置作為監控與保護網域的防禦系統，為系統中保護網路安全的重要元件，分為監測模組與 OpenFlow 交換器、Controller。

監測模組主要由入侵偵測系統與 Thershold 功能組成，負責監控及以分析網路封包。本系統是利用 Snort 來做監控封包的動作，而 Snort 會將疑似攻擊的封包事件儲存於資料庫中提供做分析判斷。當攻擊事件達到一臨界值時，將會對安全政策決策系統發送警告訊息，故 Threshold 模組，由於 Snort 會將攻擊訊息儲存在資料庫中，故在此我們建立 Threshold 模組用來判斷資料庫的攻擊事件是否達到攻擊警告的臨界值，查詢資料庫資料攻擊特徵統計否有超過攻擊事件門檻值分為兩階段，如圖 3.1 所示，第一階段為執行時間 M 分鐘一次，如果超過門檻值判定為可疑事件，進入第二階段，縮短檢測時間為 N 分鐘一次，N<M，如超過門檻值判定為攻擊事件，並將攻擊事件訊息存入分析檔案，以提供 SPDS 進行分析與給予防禦的規則。

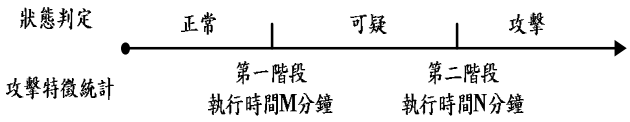


圖 3.1 攻擊特徵統計

攻擊臨界值的設定[11]，根據前 N 分鐘的網路攻擊事件量，算出 N 分鐘內平均每分鐘各攻擊特色的事件量（MEmin）。

$$\boldsymbol{Average\ Event\ Count：ME_{min}} = \frac{event\_count}{N} \quad (1)$$

公式 2 將 MEmin 與前一次門檻值乘以權重值α，進行指數平均取出新的平均門檻值 $Threshold_h$。

$$\boldsymbol{Threshold_h} = \boldsymbol{\alpha \times ME_{min} + (1-\alpha) \times Threshold_{h-1}} \quad (2)$$

公式 3 利用上述求出的值算出標準差σ_t，利用標準差進行正常範圍定義。

$$\boldsymbol{\sigma_t} = \sqrt{\boldsymbol{\alpha \times (Threshold_{h-1} - ME_{min})^2 + (1-\alpha) \times {\sigma_{t-1}}^2}} \quad (3)$$

以公式 2 算出平均門檻值，代表的是平均正常攻擊事件量，針對如何判斷公攻擊事件量已經為不正常，本論文是利用公式 4 求得的 $High\ Threshold$進行判斷，公式 4 $Threshold_h$加上β乘以標準差σ_t，β乘以標準差σ_t定義出正常範圍，β代表正常範圍的常數參數，而常數參數β的挑選會影響到誤判率。

$$\boldsymbol{High\ Threshold = Threshold_h + (\beta \times \sigma_t)} \quad (4)$$

變動攻擊的臨界值的特點在於偵測攻擊敏感程度較高，攻擊事件量超過$High\ Threshold$判定為可疑事件並且縮短觀察時間，攻擊事件量下降低至 $Threshold_h$ 時解除警報，而攻擊事件量介於$High\ Threshold$ 與 $Threshold_h$之間時為觀察期，雖然判定會是正常但並不會解除警報，如圖 3.2 所示。

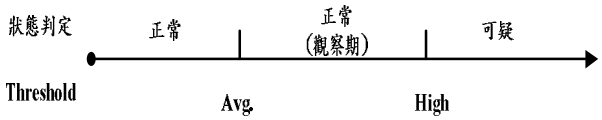
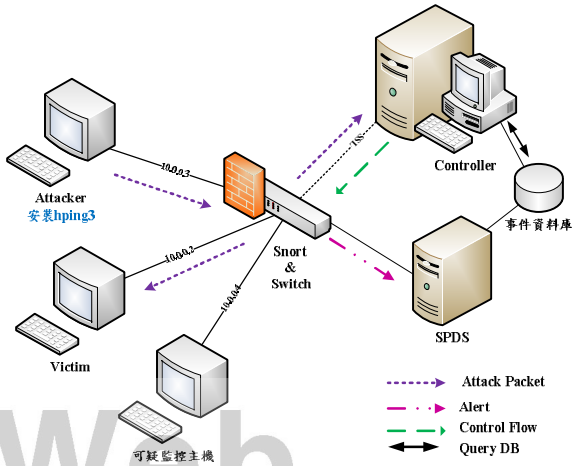


圖 3.2 門檻值判斷

安全政策決策系統，作為網路安全事件決策與管理防禦系統。該系統主要接收防禦系統的監控警報訊息，並分析警報訊息，然後根據警報訊息內的資訊進行防禦政策決策，或是驗證未確認的新型網路攻擊，防禦政策決策針對事件的攻擊類型與客戶的需求之 SLA 進行決策出相對應的防禦政策，安全政策決策系統內部元件主要包含安全政策決策模組與防禦規則更新模組。

四、 系統運作流程

使用 OpenFlow 為平台以實現網路安全防禦系統，將對整體實驗流程、實驗方式及各模組的程式流程進行說明，透過網路攻擊工具測試整體系統的運行與成果。。此實驗環境如圖四所示，Mininet 建置的 OpenFlow 網路模擬平台， 在此環境上架設了 Snort、SPDS，攻擊方為 10.0.0.3，攻擊目標為 10.0.0.2，進行攻擊為一秒發送 100 個 SYN 封包。

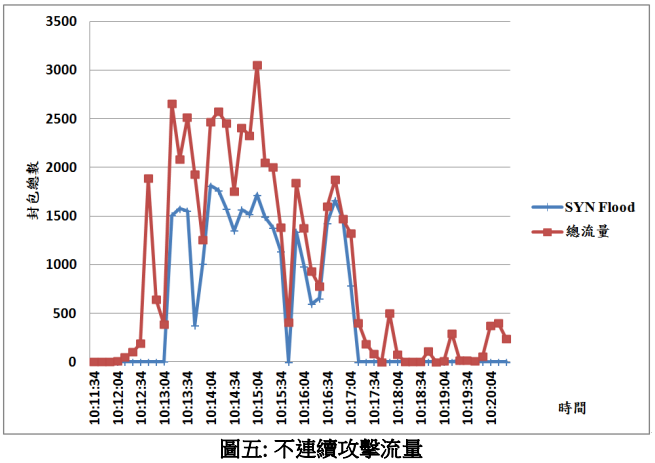


圖四:實驗環境圖

目前是使用 DoS 攻擊之中常見的 SYN Flood 攻擊做為實驗測試，當攻擊發生時會由 IDS(Snort)通知安全政策決策系統(SPDS)，當 SPDS 確定攻擊時，會更改 Black List，Controller 會根據 Black List 處理封包，當比

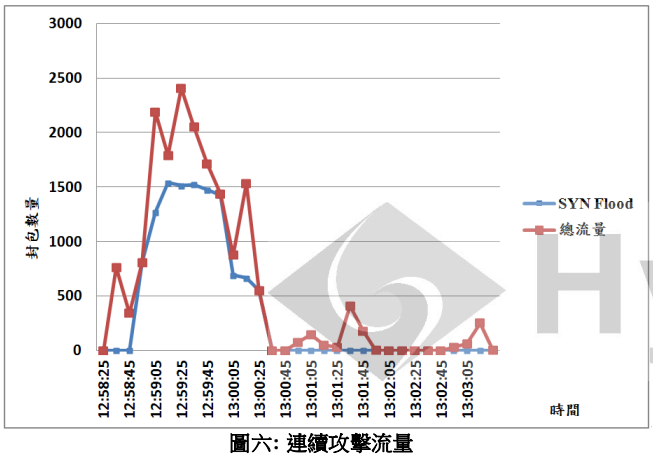
對封包特徵符合就會阻斷該封包。

當事件判斷為 2 時，進行該攻擊封包的阻擋，經過兩次門檻值的統計都超過 High Threshold，SPDS 就會將規則寫入防禦事件資料庫，OpenFlow Controller 阻擋封包。攻擊為進行攻擊為一秒發送 100 個 SYN 封包。由於實驗環境很單純，流量變化不大，但可以看到當 13 分攻擊流量進入時，封包數飆高一直持續到 17 分攻擊流量被阻擋掉。攻擊持續四分鐘被阻擋掉。當超過第一階段攻擊門檻值，會經過一分鐘進入第二階段統計攻擊門檻值，當攻擊 Alert 的數量沒超過第二門檻值會持續一段時間進行統計觀察攻擊的變化。以時間軸來看，當攻擊進行時，是非連續性的，在第一次攻擊門檻值統計兩分鐘內超過了攻擊門檻值，等待一分鐘後進入第二次門檻值統計，在兩分鐘內超過了攻擊門檻值，約四分鐘的反應時間是合理的。



圖五: 不連續攻擊流量

而圖六，x 軸為時間，y 軸為封包數，攻擊為連續攻擊，不停止持續大量灌攻擊封包，攻擊發生時為 58 分左右，從表 5.6 可以得知 SPDS 增加防禦規則於時間 13:00:19，持續到時間 13:00:25 時 SYN Flood 流量下降為零， 整體反應時間從發生攻擊到阻擋成功時間約為 2 分鐘，比第一次實驗更縮短時間，這是跟門檻值的變化以及攻擊事件持續的時間有關係，第一次攻擊為不連續攻擊，所以門檻值被提高以及觀察期變長；而第二次，大量攻擊造成 Alert 數量快速增加，很快就超過兩次門檻進行防禦，所以反應時間比第一次實驗快速。而實驗的結果都證明此系統是可以有效阻擋攻擊。



圖六: 連續攻擊流量

五、 結論

本論文參考[2][3]所提出的系統架構根據應用的環境與服務之需求來設計修改系統，實現於 OpenFlow 平台。運用 OpenFlow 平台進行安全管理與防護，並提供一個整合型安全防護機制以提高網路安全，OpenFlow 交換器、控制器負責依決策結果進行防禦動作，並結合入侵偵測系統監測網路情況，且建立安全政策決策系統，對攻擊事件進行分析與決策。

以防禦 DoS 攻擊進行案例說明，並且透過 OpenFlow 模擬進行測試，根據實驗結果，證實本論文 Threshold 模組的兩階段門檻值可以動態的依照攻擊行為制定門檻，且將攻擊訊息存分析檔案啟動 SPDS，SPDS 自動的決策出規則，再透過 OpenFlow Controller 和 OpenFlow Switch 快速檢查出封包是否符合防禦規則，有效控制封包的流動，且系統是可以進行決策且有效阻擋 DoS SYN Flood 攻擊，達到自動防禦的目的。

參考文獻

[1] 台灣電腦網路危機處理暨協調中心，http://www.cert.org.tw/news/
[2] 魏宇翔 "以服務等級協定為基礎的網路安全防禦系統之防禦資源管理機制研究", 國立中正大學電機研究所碩士論文, 2011
[3] 余孟儒, "以服務等級協定為基礎的網路安全聯防策略管理之研究與實作", 國立中正大學電機研究所碩士論文, 2010.
[4] . N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker, and J. Turner," Openflow : Enabling Innovation in Campus Networks",ACMSIGCOMM Computer Communication Review, Vo1 38, pp.69-74,April 2008.
[5] Openflow :Openflow Switch Specification 。http://www.Openflow.org/documents/Openflow-spec-v1.1.0.pdf 。
[6] 彭士家,"使用Openflow交換器偵測Botnet受害者與通知機制",國立中央大學資訊工程研究所碩士論文,2010
[7] 黃勝獅,"使用Openflow交換器分析偵測殭屍網路",國立中央大學資訊工程研究所碩士論文,2010
[8] R. Braga, E. Mota, and A. Passito, "Lightweight DDoS flooding attack detection using NOX/OpenFlow," in Local Computer Networks (LCN), 2010 IEEE 35th Conference on, 2010, pp. 408-415.
[9] Y. Chu, M. Tseng, Y. Chen, Y. Chou, and Y. Chen, "A novel design for future on-demand service and security," in Communication Technology (ICCT), 2010 12th IEEE International Conference on, 2010, pp. 385-388.
[10] K. Hyojoon and N. Feamster, "Improving network management with software defined networking," Communications Magazine, IEEE, vol. 51, pp. 114-119, 2013.
[11] K. Goto and K. Kojima, "Network intrusion and failure detection system with statistical analyses of packet headers," in Systems Engineering, 2005.ICSEng2005. 18th International Conference on, 2005,