低速阻斷服務攻擊之偵測與防禦

陳哲鋒　　賴義鵬
國防大學理工學院資訊工程學系
c0963258235@yahoo.com.tw
yopolai@gmail.com

摘要

目前學者提出防禦低速阻斷服務攻擊的方法有 RST、RAI 等方法，這些防禦方式僅能防護攻擊者惡意佔據等待佇列之攻擊，而無法防禦攻擊者針對系統計算資源之攻勢，此種攻勢使合法使用者需花費較長時間等待，超出人類對服務延遲之容忍平均值，使合法使用者放棄等待該服務達到類似阻斷服務之攻擊。本研究提出以觀察存取頻率之判斷方法，另考慮優先權之概念以進一步提升分散式低速阻斷服務攻擊之防禦效果。本文分析之範圍為網頁服務，故以使用者容忍時間為頁面回應之最大等待時間，即超過該容忍時間則對多數使用者而言，視為服務之阻斷。目前依網路資訊雜誌針對人類對回應時間最大容忍調查顯示，最大容忍等待時間為 8 秒鐘，在未使用本研究所提出防護方法防禦前，當網路服務系統遭受強度攻擊時，合法使用者能夠於容忍時間(8 秒)內存取成功之次數約為 1.8%，然於配備防禦機制後，合法使用者存取成功率能夠提升至 96.6%，相當於提升了 50 倍以上之存取成功率。
關鍵詞：阻斷服務攻擊，低速阻斷服務攻擊。

Abstract

There are many defense methods on low rate attacking proposed for making legal users access the server resources. Actually attacker can send requests to consume a lot of resources of the system, so legal users need waiting for a long time to get the response from servers. That is a kind of denial of service attacks. This thesis proposes the defense methods by observing the frequency of the user accessing times. Furthermore, we introduce the concept of priority to further obstruct the distributed low rate attacks. The maximum waiting time is assumed as the user response time tolerated. If the responding time exceeds the tolerate response time, the denial of service attacks achieved. According to the current network information magazine, the human maximum tolerate request time is 8 seconds. Without using the proposed defense methods, only 1.8% legal users can access servers. With the proposed defense mechanism, legal users access rate increases to 96.6%. It is about 50 times in increase. This paragraph describes the major work in your paper.

Keywords: Denial of service, Low-rate denial of service, Defending system.

1. 前言

由於網路的便利性讓其普及的速度急速增加，依據 2012 年 Internet Worlds Stats 調查報告中指出，2012 年全球線上人口數已將近 21 億人，相較於 2007 年時 11.5 億人，約成長的兩倍。隨著網路人口數之倍增，資訊安全事件亦隨之增加。由卡巴斯基實驗室所提供之資訊顯示，過去一個月(2013/4/6~2013/5/4)以來網路攻擊事件平均每天都有四百萬件左右，如何能使網路具備安全性又不影響網路便利性實為資訊人員重要之課題。

依據卡巴斯基實驗室的數據顯示眾多的網路攻擊事件中，阻斷服務所佔之比率達百分之七十以上。其攻擊原理不外乎就是要讓目標伺服器的各項資源被耗盡造成服務中斷，使合法使用者無法正常的存取以獲得服務。有部分的阻斷服務攻擊是利用發送大量封包的攻擊，防護者可透過檢查封包內容以及觀察流量變化來進行防禦。而攻擊者為規避這類之防禦機制，發展出低速阻斷服務攻擊方式，此種攻擊是利用為數不多的封包針對伺服器的緩衝區或是系統反應時間來進行攻擊，以達到阻斷服務攻擊的效果。

阻斷服務攻擊為耗盡目標系統之主機、網路資源，攻擊者利用發送大量偽冒之請求封包，導致系統資源被大量損耗[1]。這一類使用大量封包來進行之阻斷服務，目前已存在分析封包內容來判斷是否為惡意攻擊封包及利用防火牆來阻擋大量的封包流入等防禦方式。為規避上述防禦系統阻擋而衍生出新型態的阻斷服務攻擊稱之為低速阻斷服務攻擊(Low-Rate Denial of Service)簡稱 LRDoS。

低速阻斷服務的攻擊封包與正常的使用者封包無異，所以利用分析封包內容進行防禦之方式不適用於此類攻擊；此外 LRDoS 是在特定時間發送少量封包來進行攻擊，故亦無法透過觀察流量來進行偵測及防禦[2]。

針對低速阻斷服務攻擊 2007 年 Gabriel Maciá-Fernández 等人提出使用 RST(Random Service Time)、RAI(Random Answer Instant)之方式，其防禦原理皆是將伺服器的回應時間隨機化，使攻擊者無法確切的掌握伺服器之運作。當攻擊者無法掌握伺服器之運作時，就無法有效的佔據伺服器等待佇列

而使服務中斷。然此防禦的缺陷在於當攻擊者不需佔滿等待佇列而是利用少量請求來大量消耗伺服器資源時，縱使合法使用者能夠進入等待佇列，卻無法獲取伺服器之資源達類似阻斷服務之效果。

本研究依據低速阻斷服務攻擊特性，提出利用使用者存取伺服器之頻率來判斷合法性。觀察存取頻率對使用者進行阻擋或是放行，避免攻擊者因大量消耗系統資源造成合法使用者無法正常存取以達成防禦目的。

針對分散式低速阻斷服務攻擊若使用上述所提到使用觀察來源之存取，則頻率無法確實的阻擋此類攻擊。故提出使用存取優先權的概念來對每個來源進行過濾，於單位時間內若某來源之存取頻率超過系統門檻值，防禦系統會自動降低其存取優先權，使優先權較高之使用者先行存取系統資源。

2. 研究方法

針對阻斷服務攻擊已有許多防禦方式，透過檢查封包內容、觀察流量變化皆能夠有效的偵測出阻斷服務攻擊。而低速阻斷服務攻擊所使用之封包與正常無異且發動攻擊時之封包數量少，以目前的防禦方式是不能夠進行阻擋。

2.1 新式低速阻斷服務攻擊

低速阻斷服務攻擊的方式是針對如何讓正常的使用者能夠免於因為攻擊者持續的佔據等待佇列而造成正常使用者無法進入來獲取資源。若等待佇列未被攻擊者佔滿，但攻擊者的請求會造成伺服器運算資源大量耗損，讓合法使用者雖能進入等待佇列，卻無法在一般使用者最大容忍等待值時間內獲得伺服器回應，對一般使用者而言將達到類似阻斷服務攻擊的效果。因此本研究針對等待佇列未被攻擊者所占滿，正常使用者仍然可以進入佇列中，然而卻因為攻擊者的請求造成系統資源的大量損耗，使得正常使用者需耗費更多的等待時間來獲取資源，而達到類似 DoS 之效果。

本研究之等待時間設定是依據網路資訊雜誌[3]中提到，2000 年時人們對於空白網頁的容忍時間為 8 秒鐘，2010 年時更會降低為 3 秒鐘以下，如圖 1，2012 年時統計全球個人電腦下載網頁的時間約為 6 秒鐘，而手機下載網頁的時間約為 9 秒，因此本研究取平均值 8 秒為為一般使用者的最大容忍等待時間。

這一類的攻擊方式可利用單一攻擊來源造成 LRDoS 之效果，也可以發送更複雜的多攻擊來源造成 LRDDoS 之效果。對於這兩種不同的攻擊來源數之防禦方式亦會有所不同，本研究主要從偵測 LRDoS 攻擊，與其防禦方式為，而後推展到該如何偵測 LRDDoS 以及提出相對應之防禦方式。

圖 1 使用者容忍時間圖[3]

2.2 設計構想

由於低速阻斷服務攻擊的特性與傳統阻斷服務攻擊之特性不同，其整理的資料見表 1。

表 1 低速阻斷服務攻擊特徵差異表

	偽冒位置的阻斷服務攻擊	低速阻斷服務攻擊	分散式低速阻斷服務攻擊
來源數量	多重來源	單一來源	多重來源
封包數量	持續發送大量封包	非持續發送大量封包	非持續發送大量封包
封包內容	不同於正常	與正常無異	與正常無異
來源位置	偽冒	真實	真實

對一般的防禦設備而言，原本的阻斷服務攻擊是利用大量的請求來癱瘓目標伺服器之網路系統，或是大量消耗伺服器本身之硬體資源，所使用的封包和一般的封包有所差異，藉由分析封包內容或是觀察一段時間內封包的流量，判斷請求的來源是否為正常使用者或是攻擊者，再針對此來源放行或阻擋來進行防禦。然而，低速阻斷服務攻擊所發送的封包因需有伺服器正常的回應，故需使用與一般正常無異的封包，而且低速阻斷服務攻擊的方式是在關鍵時間點送出請求封包來癱瘓目標伺服器，故不需同原本的阻斷服務一樣，需持續發送大量封包來癱瘓目標。因此若使用原本的防禦設備來進行防禦，會發現到低速阻斷服務攻擊的封包內容、發送之請求封包數量都和正常的使用者無異，唯一的差別就是此類攻擊時間點都是經過設計所獲得，單就封包內容或是封包數量是很難對其進行防禦。

透過攻擊者來源為真實位置這一特性，我們可以將所有的來源位置進行記錄，並且計算單位時間內同一來源存取頻率，來判斷這一類存取是正常或是惡意的存取。防禦示意圖如圖 2 所示。

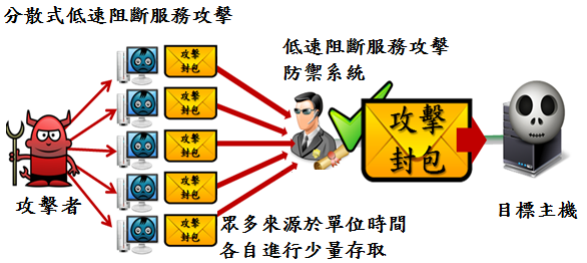
(a)防禦系統阻擋單一攻擊來源大量存取

(b)防禦系統允許單一來源正常存取

圖 2 防禦 LRDoS 示意圖

若攻擊的來源由單一轉變為多重來源時，縱使攻擊強度相同，當所有的攻擊緒全部被分散到眾多的來源之中，導致上述利用來源存取次數以判斷是否為正常使用者之防禦系統失效，因為每一個攻擊的來源其單位時間的存取量皆在系統啟動門檻值以下，故防禦機制並不會被啟動。當此多重來源的攻擊緒於同一段時間內到達伺服器，最後匯集的攻擊強度和原本無異，仍會造成伺服器因大量系統資源遭消耗而癱瘓，如圖 3 所示。

(a)防禦系統阻擋單一攻擊來源大量存取



(b)防禦系統無法阻擋眾多攻擊來源少量存取

圖 3 LRDDoS 癱瘓防禦系統示意圖

2.2.1 測試網站之建立

本研究於 Windows Server 2003 之 IIS 6.0 建立測試網站，以實作出這一類消耗系統資源之低速阻斷服務攻擊方式。當使用者連線進入此網頁時，伺服器會隨機代入一個值開始進行數學運算，而每次使用者請求所需回應時間約為 1 秒鐘。透過此網頁能模擬出伺服器為回應使用者請求時會消耗計算資源，若攻擊者能夠掌握伺服器回應時間，就能夠以少量封包在系統完成每次運算後再次提出請求，造成系統持續處於高負載狀態，使其他合法使用者無法正常的存取系統資源。

2.2.2 攻擊測試程式建立

為模擬單一來源攻擊者利用少量的封包來對目標伺服器進行存取設計了攻擊測試程式，在此程式中攻擊者可以設定要攻擊的次數、每次發送的攻擊封包數量以及每波攻擊的間隔時間。

針對模擬多重來源之攻擊者之攻勢，本研究設計簡易的 Master 與 Bot 之攻擊程式，透過 Master 可以選擇同一時間要發動多少 Bot 來進行攻擊。而每一部 Bot 都可以針對不同的攻擊模式來設定攻擊的次數及間隔。為達到同一時間多個 Bot 同步攻擊，本研究使用 VMware 來模擬多部 Bot 電腦，並且使用 Master 程式來對多部 Bot 電腦進行攻擊指令下達如圖 4。

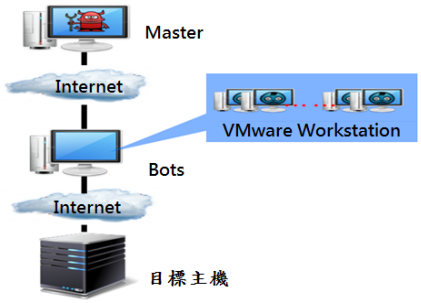


圖 4 多來源攻擊實驗架構圖

本實驗架構圖設計之目的是要模擬當攻擊緒分散至多個來源後，會導致原本防禦 LRDoS 之防禦演算法失效。在此架構之下發動攻擊所產生的封包量不大，對於網路頻寬之影響有限。而低速阻斷服務攻擊目的是為消耗目標主機之系統資源，透過本實驗架構所造成的攻擊效果確實能達此目的。

2.2.3 連線測試程式建立

為驗證攻擊時正常使用者之存取成功率故撰寫了測試連線程式，在設定執行次數、週期、等待時間後按下「開始測試」鍵，隨即會針對使用者所設定的各項參數進行連線測試。若測試週期為 10 秒、等待時間為 8 秒、測試次數為 20 次，表示每 10 秒鐘會對目標網頁伺服器進行存取，若該網頁伺服器能在 8 秒鐘內回覆則判定為成功，連線測試程式中成功率計算之關鍵因素在於「等待時間」參數之設定，若時間設置過長則連線成功率會隨之增加，反之則成功率會下降。

2.2.4 防禦演算法設計

本研究主要針對兩種不同來源數量之低速阻斷服務攻擊進行防禦，故所使用的防禦演算法亦有所不同，然而最重要的防禦關鍵點在於攻擊者為能夠獲得伺服器之回應，因此其所使之來源位置皆為真實。利用此特性設計出防禦方式。

2.2.4.1 LRDoS 防禦系統

針對單一來源之攻擊本研究提出利用來源位置為觀察目標，持續觀察各個來源於單位時間內存取的頻率，將存取次數過於頻繁之來源進行阻擋。對於正常的使用者之行為而言不會在短時間內重複且頻繁的存取同一頁面，故利用存取頻率當作是一個門檻值來限制過於頻繁之存取。此一門檻值可被防護的系統資源規格進行調整，來達成最佳的防禦效果。

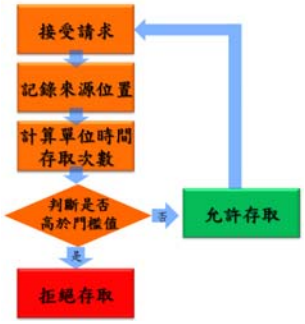


圖 5 防禦 LRDoS 流程圖

2.2.4.2 LRDDoS 防禦系統

防禦 LRDoS 方式並不適用於多攻擊來源 LRDDoS 之防禦，故將原本的防禦方式再結合上存取優先權之概念，創造出加強型防禦系統。透過持續觀察單位時間內存取此系統之數量，來決定防禦系統是否啟動。此門檻值為伺服器最大處理效能，若存取系統之總數量達門檻值時，防禦系統便會啟動並針對每個來源給予存取的優先順序。於單位時間內曾存取伺服器資源的使用者，其下次存取的優先權會較從未存取之使用者低，使未曾存取之使用者能較快獲得資源。

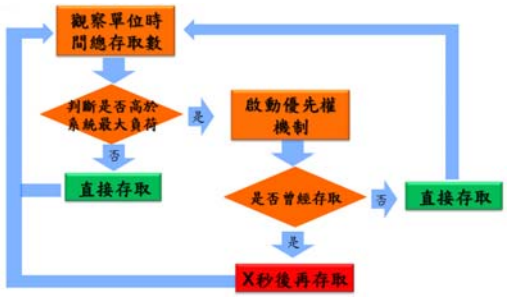


圖 6 防禦 LRDDoS 流程圖

3. 實驗結果及分析

本章節以測試網站做為攻擊目標利用攻擊程式進行攻擊，並使用連線測試程式來驗證攻擊之效能以及配備防禦後之效果。

3.1 實驗參數設定

比較架設防禦系統與未架設防禦系統之使用者成功存取次數。(8 秒內伺服器對使用者回應即為成功存取)表 2 為連線測試之各式參數設定。

表 2 連線測試參數表

總攻擊時間	1500	秒
攻擊間隔	4~10	秒
攻擊緒數量	1~7	個
使用者數量	5	位
使用者存取週期	10	秒
使用者存取次數	100	次
使用者等待時間	8	秒

依據TANet對於全國中小學進行網路服務連通率測試定義說明，該測試為定期對某校發送 10 個封包，依據該校回傳之封包數量判斷該校網路之連通率，表 3 為 2013/3/13 台北市各國中小網路連通率之數據，該日台北市 240 所學校的網路服務可連通率為 95.7755%。而本實驗之驗證成功存取之方式和上述之連線測試方式無異，故設定成功存取頻率目標為 90%(含)以上表示伺服器為正常運作，不受攻擊等因素所影響。

表 3 台北市 TANet 網路服務可連通率日報表[4]

★★★TANet國中小學網路服務品質偵測系統-台北市日報表★★★

偵測統計時段：2013年03月13日

學校編號	學校名稱	網站/偵測位址	偵測方式	網路服務可連通率	網路服務回應時間
313602	市立西松國小	www.sups.tp.edu.tw	HTTP	100.0000%	0.9895ms
313601	市立松山國小	www.ssps.tp.edu.tw	HTTP	100.0000%	27.6960ms
313604	市立敦化國小	www.thps.tp.edu.tw	HTTP	100.0000%	10.9461ms
313605	市立民生國小	www.msps.tp.edu.tw	HTTP	100.0000%	62.8274ms
313606	市立民權國小	www.mcps.tp.edu.tw	HTTP	100.0000%	50.0882ms
313607	市立民族國小	www.mces.tp.edu.tw	HTTP	100.0000%	28.9100ms
313608	市立三民國小	www.smps.tp.edu.tw	HTTP	100.0000%	1.5275ms
313609	市立健康國小	www.jkes.tp.edu.tw	HTTP	100.0000%	1.4813ms
323601	市立興雅國小	www.hyps.tp.edu.tw	HTTP	100.0000%	84.7843ms
400219	國立臺灣戲曲專科學校(附中)	www.ntjcpa.edu.tw	HTTP	0.0000%	0.0000ms
401302	私立方濟中學(附中)	www.sfh.tp.edu.tw	HTTP	100.0000%	103.7957ms
401303	私立達人女中(附中)	www.trgsh.tp.edu.tw	HTTP	97.9167%	96.7580ms
411302	私立衛理女中(附中)	www.wlgsh.tp.edu.tw	HTTP	100.0000%	28.7581ms
411303	私立華興中學(附中)	www.hhhs.tp.edu.tw	HTTP	96.5278%	55.5016ms
413301	市立陽明高中(附中)	www.ymsh.tp.edu.tw	HTTP	100.0000%	0.6681ms
413302	市立百齡高中(附中)	www.blsh.tp.edu.tw	HTTP	100.0000%	5.9773ms
421301	私立鐵崗高中(附中)	www.wghs.tp.edu.tw	HTTP	100.0000%	23.3066ms
台北市240校平均值			HTTP	95.7755%	54.6471ms

3.2 LRDoS 實驗數據

在未配備防禦的情況之下，可發現當攻擊週期愈短時，所需的攻擊緒列數愈小即可以使連線成功率降至 50%以下。其原因如下，當攻擊週期為 4 秒、攻擊緒列數為 2，每 200 秒所產生的攻擊緒列為 100 次，相當於攻擊週期為 10 秒、攻擊緒列數為 5 次所產生之效果。計算方式如下：

總攻擊序列數 = 攻擊序列數 × (總攻擊時間 / 攻擊週期)

透過防禦伺服器的防禦，存取過於頻繁的使用者或是惡意的攻擊者都會被阻擋在外，避免其存取伺服器資源過多而造成系統負擔。在配備防禦伺服器後，連線成功率可以達到 90%以上，由於本防禦伺服器是當攻擊緒數量超過門檻值時才會啟動，因

此當攻擊的緒列數愈快達到門檻值時，防禦機制就會愈早啟動。

另外可發現原本連線成功率為 100%在配備防禦伺服器後亦為 100%，故本防禦機制不會造成使用者額外的負擔而降低連線成功率。

3.3 LRDDoS 實驗數據

配備 LRDoS 防禦系統之伺服器無法成功阻止 LRDDoS 之攻擊，比較數據如圖 7。

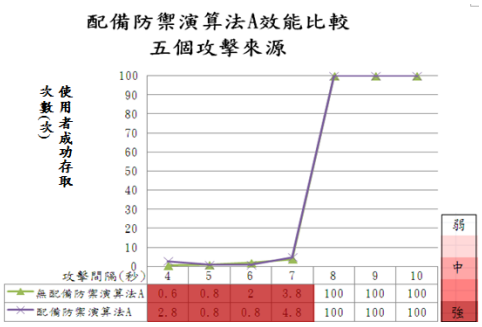


圖 7 有無配備防禦演算法 A 曲線圖

為能有效的防禦 LRDDoS 之攻擊本研究設計雙重防禦方式，此防禦方式會持續監控系統單位時間的存取頻率，當單位時間存取的頻率接近系統最大負載之門檻值時，則會啟動優先權的判斷機制來針對所有請求來源進行判斷，當某一來源於單位時間內之存取頻率高於門檻值時，防禦伺服器便會降低其存取優先權進而使其他優先權較高之使用者先行存取系統資源。與原先無防禦之效能比較圖如圖 8。

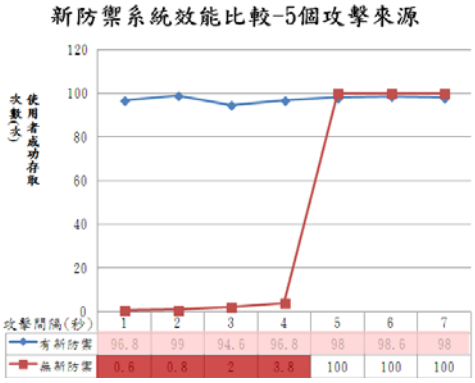


圖 8 有無配備 LRDDoS 防禦系統效能比較曲線圖

3.4 防禦系統效能分析

在無配備防禦的情況之下，當系統遭受到攻擊時，會造成中央處理器的資源大量被攻擊者所耗盡。導致一般的使用者需要花費更多的時間等待才能夠獲得伺服器的回應。雖然透過將伺服器的記憶體資源向上提升一倍，卻依舊無法獲得良好的防禦效果，故無法單就提升伺服器的系統資源來進行此類低速阻斷服務攻擊之防禦。

3.4.1 防禦 LRDoS 效能分析

在配備防禦伺服器之後，可以發現正常使用者所需等待伺服器的回應時間縮短，但是卻依舊無法達到未遭受攻擊時的速度，這是因為透過本研究所提出的防禦方式雖然可以阻擋攻擊者的攻擊行動。但基於防禦系統在一段時間後會再一次的開放攻擊者存取伺服器資源，待存取頻率過高時才會再一次的將攻擊者阻擋在外。因此，每次防禦伺服器開放攻擊者進入網頁伺服器時，又會大量耗費中央處理器資源，造成瞬間使用者所需等待的時間又增加，故平均防禦的效果能達到 96%以上，而相較於 TANet 所提供之全國中小學網路服務連通率台北市地區平均連通率為 95.7，本研究之數據已經超過其平均值。

若能將存取資源的門檻值做一良好的設定，那麼對於正常的使用者而言，存取網頁伺服器所需等待時間都會是在合理的範圍之中。

3.4.2 防禦 LRDDoS 效能分析

由於 LRDDoS 為多重攻擊來源，若利用防禦 LRDoS 之系統來進行防禦可發現效果不彰。主要原因在於當攻擊緒分散到多個攻擊來源後，對原本的防禦系統而言，每個攻擊來源其單位時間的存取次數皆低於防禦系統啟動之門檻值，因此每個攻擊來源皆能夠成功存取系統資源。當這些大量之惡意存取於同一時間抵達伺服器時，依舊會消耗伺服器之大量資源。

透過防禦系統之預先偵查單位時間存取伺服器之總次數來判斷是否啟動優先權過濾機制，若伺服器單位時間的總存取次數低於最大負載值時，表示伺服器能夠正常的進行運作，即所有使用者均能獲得服務。然而若是優先權機制過早啟動，則可能會造成部份存取次數接近門檻值之合法使用者被系統降低其存取優先權而無法存取。若過晚啟動則會造成伺服器資源大量耗損無法提供正常服務。為避免此類情況發生，本研究取系統單位時間最大負荷量作為啟動門檻值，並且持續觀察單位時間之總存取次數，使優先權機制能夠適時的啟動或關閉。如此才能有效防禦卻又不至於導致自身之阻斷服務情況發生。

門檻值之取得為觀察系統在單位時間內能夠處理多少的使用者之請求，經觀察發現若要使存取的成功率達 90%以上，則單位時間內系統之最大負載量為 33 個請求。然而若設定啟動門檻值為 33 則會造成合法使用者在防禦機制啟動之後，於單位時間內能在不受攻擊影響的存取時間降低。故本研究先將所有單位時間內合法使用者的存取次數(15 次/30 秒)扣除後，得到門檻值為 18。然而經過實驗測試，

若將防禦系統啟動之門檻值設定為每 30 秒 18 次，則合法使用者成功存取次數並無法達成預期成效。經過幾次實驗後求得當門檻值設定為每 30 秒 10 次時即可獲得預期之成效。

4. 結論

網路攻擊事件亦隨網路使用率之增加而水漲船高，依據卡巴斯基實驗室 Securelist[5]所提供之資料顯示在過去一個月(2013/4/6~2013/5/4)以來，全球每日的網路攻擊事件皆以百萬計算。在各種類型的資安攻擊事件中又以阻斷式服務攻擊為最大宗。本研究針對由阻斷服務攻擊所衍生出來的新威脅「低速阻斷服務攻擊」及其延伸之「分散式低速阻斷服務攻擊」此兩類威脅進行探討及設計相關之防禦方式。

為模擬低速阻斷服務攻擊之效果，本研究設計的相關的目標網站以及攻擊、測試之程式，其能獲得相關數據。經過實驗後發現，在未配備防禦系統時，伺服器的效能會因為攻擊而大量耗損，導致合法使用者無法正常存取系統資源。在遭受到 LRDoS 最高攻擊強度的情況之下，會造成伺服器的 CPU 使用率持續處於 100%，而合法使用者的平均存取次數卻只有 1.8%，網路使用率卻只有 0.1%(100Mbps)；而在遭受到最高強度之 LRDDoS 攻擊時，合法使用者成功存取次數為 0 次，網路使用率卻不到 1%(100Mbps)。因此若透過網路流量來偵測是否發生阻斷服務攻擊，是無法偵測出低速阻斷服務攻擊。

透過本研究提出之防禦系統可以讓伺服器遭受相同強度攻擊期間，依舊能夠提供合法使用者正常的存取。透過實驗發現在系統遭受 LRDoS 攻擊時，若能夠配備 LRDoS 防禦系統，則合法使用者成功存取的比例從原本的 1.8%大幅提升至 96.6%；而當系統遭受 LRDDoS 攻擊時，配備 LRDDoS 防禦系統之後，讓合法使用者成功存取率從原本完全無法存取之 0%大幅提升至 93.6%。

本研究利用低速阻斷服務之特性，觀察單位時間內存取系統之頻率來判斷該存取來源為合法的使用者抑或是攻擊者。並依據來源數量為單一或是分散之攻擊設計出不同之防禦系統，經實驗發現合法使用者在系統配備上防禦後皆能讓存取成功率提升 50%以上。

參考文獻

[1] David Moore,Colleen Shanno, Douglas J. Brown,Geoffrey M. Voelker, and Stefan Savage,“ Inferring Internet Denial-of-Service Activity,” ACM, Vol. 24, No.2 ,pp. 115 – 139, 2006.

[2] Gabriel Macia-Fernandez, Rafael A. Rodriguez-GomezJesus E. Diaz-Verdejo,“Defense techniques for low-rate DoS attacks against application servers,” Computer Networks,Vol. 54, No.15,pp. 2711-2727 ,2010.

[3] http://news.networkmagazine.com.tw/classification/web/2012/03/02/38107/ (2013.5.1)

[4] http://nms.moe.edu.tw/ism/(2013.3.13)

[5] http://www.securelist.com/en/statistics#/en/top20/ids/month(2013.5.7)