Journal of Science and Engineering Technology, Vol. 5, No. 3, pp. 77-85 (2009)

適用於 IPv6 無線網路芳鄰探索攻擊的防禦系統

薛來銘[1]　張阜民[2]　林建霖[3]　高勝助[3]

[1]耕莘健康管理專科學校數位媒體設計科

23143 台北縣新店市民族路 112 號

[2]朝陽科技大學財務金融系

41349 台中縣霧峰鄉吉峰東路 168 號

[3]中興大學資訊科學與工程學系

40227 台中市國光路 250 號

摘　要

在 IPv6 網路中，相同連結上的各個節點利用芳鄰探索（neighbor discovery, ND）協定來確定相鄰節點之間的關係（如確定對方是否存在、解析對方的連結層位址等）及進行基本的網路組態配置。在沒有確保連結上的節點都是可信任的情形下，此協定容易遭受惡意偽造封包的威脅，尤其在無線的網路環境下，此威脅更加難以防範。雖然 IETF 提出了 SEcure Neighbor Discovery（SEND）協定來保護芳鄰探索訊息的安全，但驗證過程需要花時間及系統資源，對於一般輕型的無線網路的裝置，造成了不小的負擔。

在本文中，我們提出一個避免 IPv6 無線網路下芳鄰探索機制被攻擊且適用於輕型無線裝置的防禦系統。藉由 IPv6 節點取得合法 IP 位址時，會先經重複位址偵測（duplicate address detection, DAD）程序來確保位址唯一的特性，本系統透過分析 DAD 訊息封包及追蹤使用者連線狀態的方式，來阻檔偽造芳鄰探索封包的攻擊。我們利用 HostAP 軟體作爲無線基地台，並修改 HostAP 軟體核心，將防禦功能植入。實驗結果顯示我們所提出系統的效能，足讓一般輕型的無線裝置皆適用於本防禦系統。

關鍵詞：芳鄰探索，重複位址偵測，網路安全

A Defensive System Against Neighbor Discovery Attacks in IPv6 Wireless Networks

LAI-MING SHIUE[1], FU-MIN CHANG[2], CHENG-LIN LIN[3] and SHANG-JUH KAO[3]

[1]Department of Digital Design, Cardinal Tien College of Healthcare and Management

No. 112, Minzu Rd., Sindian, Taipei, Taiwan 23143, R.O.C

[2]Department of Finance, Chaoyang University of Technology

No. 168, Jifong E. Rd., Wufong, Taichung, Taiwan 41349, R.O.C

[3]Department of Computer Science and Engineering, National Chung-Hsing University

No. 250, Kuo Kuang Rd., Taichung, Taiwan 40227, R.O.C

ABSTRACT

In IPv6 networks, Neighbor Discovery Protocol (NDP) is usually used to determine the relationship (e.g., the current accessibility or the link-layer address of a neighboring node) between nodes on the same link and to configure the network interface. This protocol is vulnerable to threats from spoofing packets due to the lack of a mutual trust mechanism among the communication nodes, especially in wireless environments. Therefore, the IETF has proposed the Secure Neighbor Discovery (SEND) protocol to safeguard Neighbor Discovery messages. Currently, common lightweight wireless network devices tend to reduce resource consumption, thereby conflicting with heavyweight SEND message computational requirements.

In this research, a defensive system against Neighbor Discovery (ND) attacks on lightweight devices in IPv6 wireless networks is proposed. In an IPv6 network, as a node prepares to assume a new address for its own use, it must first verify that no other node on the link uses that particular address. This procedure is accomplished by the Duplicate Address Detection (DAD) process. By implementing this feature, through an analysis of DAD packets and tracing the user's linking status, spoofing ND packets can be effectively blocked. In the proposed system, a HostAP was adopted to provide access-point functions. Thus, we modified the kernel of the HostAP for embedding the defense functions. The experimental results revealed that the proposed system is both applicable to and appropriate for the network security of lightweight wireless devices operating in IPv6 wireless networks.

***Key Words*:** neighbor discovery protocol (NDP), duplicate address detection (DAD), network security

一、簡介

在 IPv6 [5] 網路中，芳鄰探索協定（neighbor discovery protocol, NDP）[9] 取代 IPv4 中由 ARP 協定及 ICMP 協定所提供之路由探索和重導訊息的功能，並新增相鄰節點不可到達偵測（neighbor unreachable detection, NUD）、重複位址偵測（duplicate address detection, DAD）及無狀態自動組態（Stateless Autocon figuration）[11] 等功能。根據 ICMPv6 的定義，芳鄰探索協定包含五種封包格式：相鄰節點邀請（neighbor solicitation, NS）、相鄰節點公告（neighbor advertisements, NA）、路由器邀請（router solicitation, RS）、路由器公告（router advertisement, RA）和重導訊息（redirect）。透過此協定，各節點可在區域網路內取得有效的 IPv6 位址並進行基本的網路組態配置。

芳鄰探索機制能夠正確且安全地運作，在同一連結上的各節點必須互相信任，若芳鄰探索機制在未受保護的環境中，非常容易受到偽造封包的攻擊 [10]。傳送中的資料封包可能會被重新導向到惡意節點，造成資料遺失或資訊被竊取甚至癱瘓整個區域網路。芳鄰探索機制的威脅可分爲非路由相關及路由相關兩種類型。

非路由相關之威脅來自於 IPv6 節點之間藉由 NS 和 NA 訊息交換，其包括有：連結層位址重導、相鄰節點不可到達偵測失敗以及重複位址偵測 DoS。若攻擊者偽造 NS 或 NA 訊息，讓被攻擊節點在收到偽造訊息後默認且更新自己的芳鄰快取表，導致在連結層的訊框無法正確地傳，此種攻擊爲連結層位址重導；相鄰節點不可到達偵測失敗係指攻擊者監聽區域網路上所有的 NS 封包，並偽造 NA 來回應 NS，欺騙受害者宣稱目的節點尚能到達，使相鄰節點不可到達偵測的功能無法實際反應真實情況；當攻擊者監聽區域網路上所有的 NS 封包，可容易地產生具有偽造目標位址的 NS 封包來假裝重複位址偵測，或是佯裝成相同目標位址主機回應 NA 封包，讓受害節點以爲發生碰撞，造成受害者無法正常取得 IP 位址的使用權，此種攻擊稱爲重複位址偵測 DoS。

在 IPv6 環境下，主機與路由器之間藉由 RS、RA 訊息的交換，來達成尋找本地子網路的路由器、位址前綴發現、其它組態參數發現、更佳的路徑重新導向等功能。攻擊者會透過偽造 RA 封包傳送假的路由組態資訊進行攻擊，此爲與路由相關的威脅，其包含：惡意的路由器（malicious router）、假造位址前綴（bogus prefix）、假造路由組態參數（parameters spoofing）以及假造重導訊息（spoofed redirect message）。

攻擊者可佯裝爲對外的路由器（稱之爲惡意的路由器），對本地連結的主機傳送群播的 RA 訊息或回應的 RA 訊息，使本地連結的主機誤認爲其爲對外連線的路由器，以便接收所有主機對外的連線資料；假造位址前綴是指攻擊者可以經由設定 On-link 或 Autonomous 旗標以傳送包含僞裝位址前綴的 RA 訊息。當主機收到 On-link 旗標爲 1 的僞造位址前綴時，會誤認與此位址前綴的網域在同一連結上，導致主機與此位址前綴的節點通訊時，將改由直接通訊不再經由本地路由器轉送，其結果將得不到回應；若主機收到 Autonomous 旗標的僞造位址前綴，便會以此位址前綴做位址的自動組態，導致產生一個無效的 IP 位址；假造路由組態參數是指攻擊主機可佯裝成合法路由器用以僞造不同的參數傳送給連結上的主機，例如：僞造 MTU 爲很小的數值，其結果會造成網路的碎片封包過多；僞造 Router Lifetime 值設爲 0，讓合法的路由器從主機的預設路由器設定中移除；當擊者可以僞造 Redirect 訊息將任一台主機的全部或部份封包重新導向到另一個在本地連結的 IP 位址，這一類的威脅稱之爲假造重導訊息。

在有線網路的環境中，同一連結上的各節點能夠互相信任，可藉由實體線路的佈置來加以控管。但對於公用無線網路而言，即使是提供 802.1x 或 802.11i 的 AAA 機制的無線網路環境，各無線節點之間仍可能互不信任 [2]。在 IPv6 的網路，雖然規定需強制使用 IPSec [7]，使得網路第三層以上的協定安全得已被保護，包括芳鄰探索協定的訊息。但利用 IPSec 的方式來保護芳鄰探索訊息，只能透過手動的方式來設定加密金鑰，相當麻煩且不切實際，更違反 IPv6 隨插即用的特性。

在另一方面，IETF 提出了 SEcure Neighbor Discovery（SEND）[1] 協定，可以讓芳鄰探索訊息具備自我認證的特性，即使在互不信任的區域網路內亦可完成芳鄰探索的工作。SEND 機制實作於終端節點，各節點必需產生一組公鑰和私鑰，再利用 Cryptographically Generated Addresses（CGA）[3] 產生 IPv6 位址以保證其位址擁有權，並在芳鄰探索封包新增數個選項來防禦攻擊。CGA 產生位址的方法是將自己公鑰、MAC、Prefix 和其它參數全部連結起來然後經過 SHA-1 雜湊函數來產生 IPv6 位址的 interface identifier 部分，讓公鑰、MAC、Prefix、其它參數與 IPv6 位址產生關聯，如圖 1 所示。同時，只有真正的 IPv6 位址

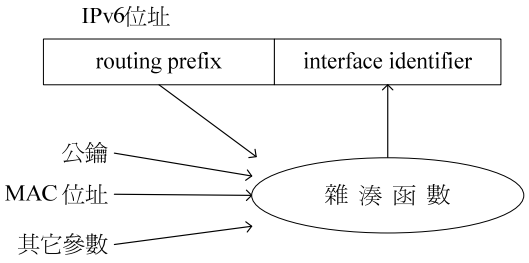

圖 1. 產生 CGA 位址

擁有者才有對應此 IPv6 位址的私鑰。

SEND 定義了 4 種芳鄰探索選項：CGA、RSA Signature、Nonce 與 Timestamp，讓接收方驗證是否爲合法的芳鄰探索訊息。傳送方會將公鑰放在 CGA 選項；整個芳鄰探索訊息以私鑰做簽章則放在 RSA Signature 選項，此選項必需放在所有的選項的結尾；Nonce 與 Timestamp 選項則是用來防止重送攻擊。當有啓動 SEND 的節點收到芳鄰探索封包時，若不含依 SEND 規定要附加的選項時會直接丟棄，若符合規定就會針對來源端 IPv6 位址及各附加的選項一一驗證。而這些驗證過程是需要花一些時間的，且 SEND 的機制並未普及化，對於 Non-SEND 的節點亦無法提供保護。

針對此問題，Beck 等人於 2007 年提出 NDPMon 的軟體來監控芳鄰探索協定 [4]。該系統是應用於一般 IPv6 環境下，監看芳鄰探索協定，若有攻擊產生則回報。在實作方面是透過修改系統核心來達成目標。但若在 IPv6 無線網路下芳鄰探索機制遭受攻擊時，該系統則不適用。再者該系統著重監看芳鄰探索協定及回報攻擊，並無法即時避免攻擊。在本論文中，我們設計與實作一個適用於 IPv6 無線網路芳鄰探索攻擊的防禦系統。我們利用在 IPv6 網路環境中，不論是任何方式設定新的位址之前，必須先完成重複位址偵測的特性，來確定 IPv6 位址的擁有權是否合法。在此系統中，我們收集所有無線媒介傳送的芳鄰探索封包，進行封包分析及行爲追蹤。防禦系統會阻擋被識別爲僞造的封包，使其無法對其他有線或無線的節點 進行攻擊。爲了驗證所提出防禦系統的可行性，我們利用 HostAP [8] 軟體作爲無線基地台，並透過修改 HostAP 軟體的核心，將防禦功能植入。HostAP 是在 Linux 平台下用來驅動具有 Intersil's Prism2/2.5/3 晶片組的無線網卡的驅動程式，此驅動程式可

以讓網路卡支援無線基地台的功能。此外我們亦將 SEND 機制與本系統的差異性進行效能實測比較，實驗的結果證明本系統擁有較佳的效能，讓一般輕型的無線裝置不需增加額外的負擔即可適合於本防禦系統。

二、系統設計與實作

（一）系統架構

在此系統中，我們以 Linux 爲作業平台，使用 HostAP 軟體來實現無線基地台的功能。我們在 HostAP 驅動程式中增加 ND 防禦模組（neighbor discovery defense module, NDDM）來阻擋僞造的攻擊；此外在 Linux 的使用者層設計 ND 管理模組（neighbor discovery management module, NDMM），對內負責與 ND 防禦模組作溝通設定，對外負責輸出記錄檔至管理站（mgmt station），並提供管理介面讓管理者可以透過管理站設定 NDDM 相關參數、及與其它同區域網路的 ND 管理模組分享合法主機的資訊。本防禦系統幾乎不需增加無線裝置的負擔下依然能有效率的阻擋攻擊。整個防禦系統架構圖，如圖 2 所示。

（二）ND 防禦模組

ND 防禦模組包含接收 ND 封包過濾流程、DAD 狀態更新模組 (II) 及修改後的 ap_free_sta() 函數。我們修改原有 HostAP 的接收封包流程，在封包即將選擇 Data Device 或 TCP/IP Protocol Stack 傳送出去之前，加入接收 ND 封包過濾流程以阻擋僞造的 ND 封包。我們修改原有 HostAP 的傳送封包流程，在封包即將往 Radio Device 傳送出去之前，加入 DAD 狀態更新模組（II）以更新 IPv6_Status 表。我們修改 HostAP 釋放 Station（當 Station 離開時）的函數 ap_free_sta()，於 HostAP 釋放 Station 時，加入刪除該 Station 在 IPv6_Status 所留下來的記錄之功能。透過這些功能的增加與修改，僞造的 ND 封包得以有效的被阻檔。子模組加入接收封包流程、傳收封包流程及 ap_free_sta() 加入 ND 防禦模組之後的流程，如圖 3 及圖 4 所示。

ND 防禦模組維護二個表格，IPv6_Status 和 Legal_RA。IPv6_Status 記錄 IPv6 位址與網卡位址的對應及狀態，Legal_RA 記錄合法路由器公告的內容。IPv6_Status 主要用來追蹤 IPv6 擁有權的狀態，其中包括阻擋、DAD 測試以及放行三種狀態，除了 DAD 封包放行外，其它未加入 IPv6_Status 表的來源 IPv6 位址將會被阻擋，只有成功經過 DAD 程序的 IPv6 位址（1 秒後未收到同 IP 位址的 NS 或合法的 NA，即由 DAD 測試狀態轉爲放行狀態，因 RFC 2461 [9] 定義，節點送出邀請最多會等待 RETRANS_TIMER 時間，預設爲 1 秒），才能通行，如此可以保護經過 DAD 程序取得 IPv6 位址擁有權不被攻擊。圖 5 爲本系統追蹤 IPv6 位址擁有權的狀態圖。

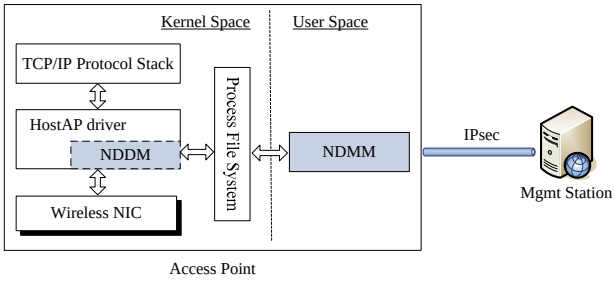

圖 2. 防禦系統架構圖

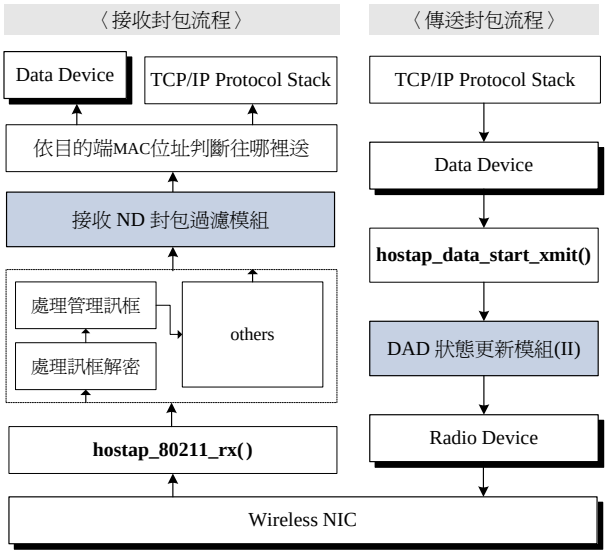

圖 3. 子模組加入接收封包流程、傳送封包流程

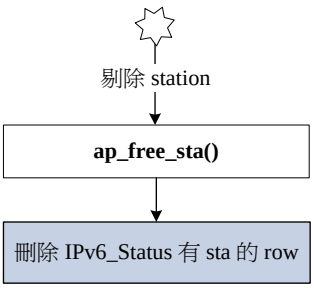

圖 4. ap_free_sta() 加入 ND 防禦模組之後的流程

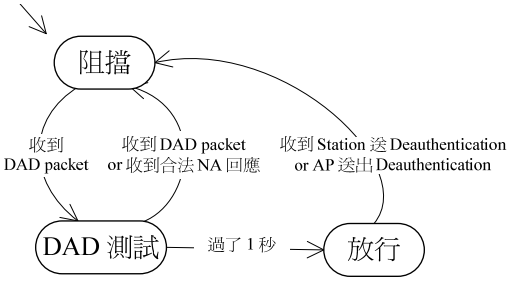

圖 5. 追蹤 IPv6 位址狀態圖

舉個例子來說，當 NDDM 收到 DAD 封包，內容是

NS: [::] multicast to FF02::1:FFAF:0E63 "Who has FE80::0240:05FF:FEAF:0E63"

我們 IPv6_Status 表會增加一筆記錄，且將 Status 設爲「DAD TEST」，如表 1 所示。

當系統過了一秒，DAD 程序完成之後，Status 會自動更改爲「PASS」，如表 2 所示。

Legal_RA 表（欄位有 IP, MAC, Hoplimit, Lifetime, Prefixes, MTU, etc.）讓區域網路的管理者透過安全的管道由 ND 管理模組設定合法的 RA 資訊。在一般 WLAN，路由器透過 AP 於有線網路端傳送 Router Advertisement，所以合法的 RA 不會從無線的媒介進入，AP 在無線網卡收到 RA 時可以直接阻擋。舉例來說，我們建立一個 IPv6 的無線區網，這個 WLAN 透過 IPv6 路由器與 Internet 連接，此路由器的 link-local 的 IPv6 與 MAC 位址是 FE80::218:F3FF:FEE9:9155 / 00:18:F3:E9:91:55，分配給 WLAN 區網的 Prfix 爲 2001:288:5001:10::/64，所以我們可以經由管理者設定合法授權的 RA 至 NDDM 的 Legal_RA 表，如表 3，其中設定爲 0 的參數代表不由路由器指定，如此我們 NDDM 就可以阻擋僞造的 RA 想要藉由 AP 傳送給其它 Station。

收 ND 封包過濾流程是本系統最關鍵的流程，針對封包進行分析及過濾，其流程如圖 6 所示。

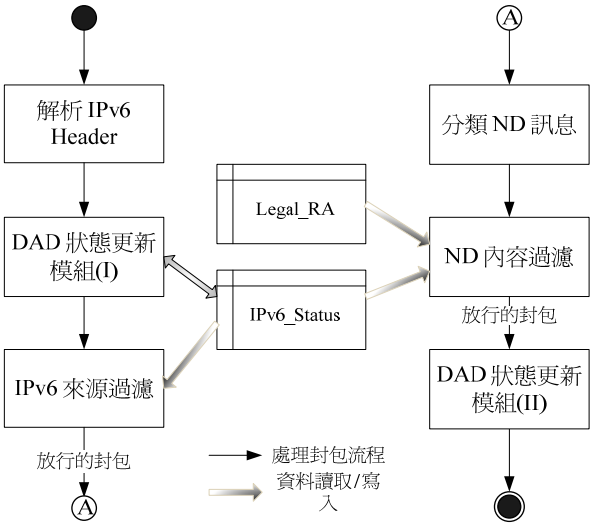

圖 6. 接收 ND 封包過濾流程

表 1. IPv6_Status 加入一筆 DAD 測試記錄

IP	MAC	Timstamp	Status
FE80::0240:05FF:FEAF:0E63	00:40:05:AF:0E:63	1192881888	DAD TEST

表 2. IPv6_Status DAD 成功記錄

IP	MAC	Timstamp	Status
FE80::0240:05FF:FEAF:0E63	00:40:05:AF:0E:63	1192881889	PASS

表 3. Legal_RA 儲存合法的 RA 記錄

IP	MAC	Hoplimit	RouterLifetime	ReachableTime	RetransTime
FE80::218:F3FF:FEE9:9155	00:18:F3:E9:91:55	64	1800	0	0

Prefix	PrefixLen	On-link	Autonomous	ValidLifetime	PreferredLifetime	MTU
2001:288:5001:10::	64	True	True	2592000	604800	0

1. 解析 IPv6 Header：對 IPv6 標頭的做基本解析，檢查 ICMPv6 的 checksum 是否正確，獲得 IPv6 標頭的資訊以供後續步驟使用。
2. DAD 狀態更新模組（I）：對於將要進行 DAD 程序及通過 DAD 程序的 IPv6 與 MAC 對應以及狀態記錄在 IPv6_Status 表，並將異動 IPv6_Status 表的記錄輸出至 Process File System 的 nddm_log，以供 ND 管理模組收集且輸出至管理站。
3. IPv6 來源過濾：依據 IPv6_Status 表資料，阻擋非放行及沒記錄之封包，將阻檔的記錄輸出至 Process File System 的 nddm_log。
4. 分類 ND 訊息：先分析 ND 訊息，得到 ND 封包各個欄位的資訊後，然後依 NS、NA、RS、RA、Redirect 五種分類，使用不同的過濾方式，如下個步驟所述。
5. ND 內容過濾：NS、NA、RS 訊息用 IPv6_Status 表來當過濾的標準，阻擋 IPv6_Status 狀態記錄爲非放行或沒 IPv6_Status 記錄之封包，RA 訊息用 Legal_RA 表爲過濾的標準，將阻檔的記錄輸出至 Process File System 的 nddm_log。
6. DAD 狀態更新模組（II）：若有合法的 NA 對 DAD 回應，代表 DAD 失敗，所以在 IPv6_Status 表刪除 IPv6 與 MAC 的對應，並將異動 IPv6_Status 表的記錄輸出至 Process File System 的 nddm_log。

本系統追蹤 IPv6 位址的狀態主要是在 DAD 狀態更新模組（I）、（II）。DAD 狀態更新模組（I）用來偵測及記錄 DAD 與 DAD 成功的 IP 與 MAC 的對應，而 DAD 狀態更新模組（II）用來偵測 DAD 失敗的情況。圖 7 爲 DAD 狀態更新模組（I）、（II）的詳細流程圖。

（三）ND 管理模組

ND 管理模組主要負責對內控制 ND 防禦模組，對外則輸出 ND 管理模組的記錄檔至管理站。此外 ND 管理模組提供管理介面給管理站設定 ND 防禦模組的相關參數及與其它同區網的 ND 管理模組分享合法主機的資訊。ND 管理模組包含三個子模組：Log Recorder、NDDM Controller 及 Mgmt Station Communication。Log Recorder 會週期性的去存取 Process File System 的 nddm_log 檔，並將存取到的記錄，經由 Mgmt Station Communication 模組傳給管理站，存入資料庫。NDDM Controller 模組的主要功能是提供管理者可以

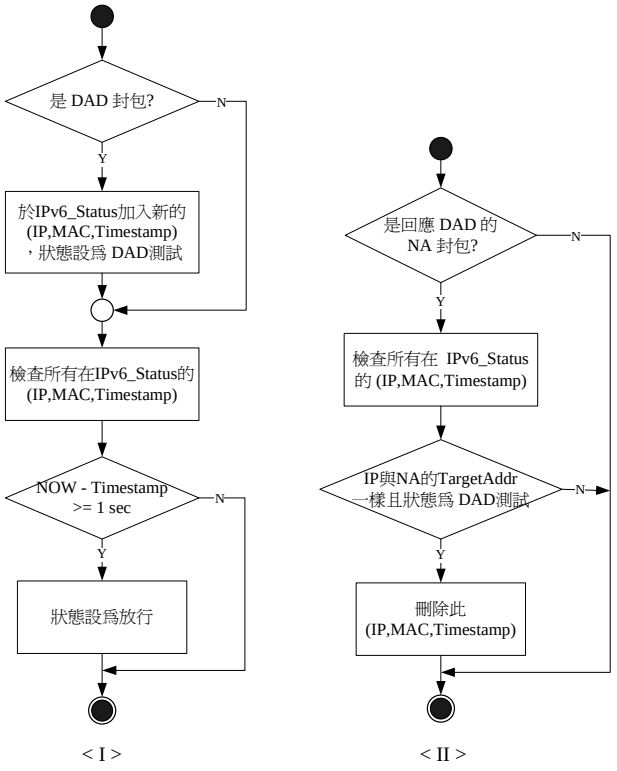

圖 7. DAD 狀態更新模組（I）、（II）流程圖

經由管理站來手動設定 NDDM 中的 IPv6_Status 與 Legal_RA 兩個表格，以控制 NDDM 的過濾封包的行爲。Mgmt Station Communication 模組主要是處理 ND 管理模組與管理站之間的溝通訊息。ND 管理模組的架構圖，如圖 8 所示。

三、安全性評估與效能測試

爲了驗證本系統的可行性，我們建立一個實驗環境來針對本系統的安全性與效能進行評估與測試。在安全性評估的部份，我們透過封包的流程分析，展示我們的系統如何對抗

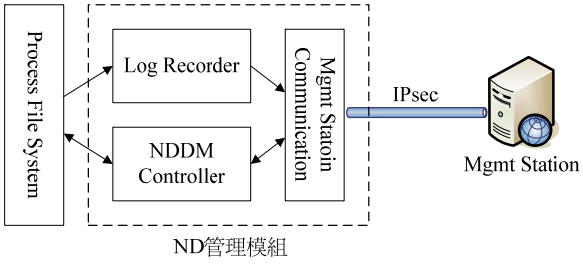

圖 8. ND 管理模組架構圖

芳鄰探索攻擊的威脅；在效能測試的部分，我們將本系統與目前唯一實作 SEND 的軟體 Open Source SEND Project [6] 做實際的效能比較。整個實驗環境，如圖 9 所示。在實驗環境中，區網透過具有 IPv6 功能的路由器與外部網路連接，有線網路部分包含一個 Host D 節點與使用 HostAP 所架設的無線基地台，無線網路部分包含無線裝置 Station A、Station B 與 Attacker C 與 AP 作連線。

（一）安全性評估

在開始封包流程的分析前，先說明之後圖中的表示方法。

虛線箭頭 - - - →：由 Station 傳給 AP 的訊框

實線箭頭 ——→：由 AP 傳給 Station 的訊框

丟棄封包 ✕：AP 將收到的封包丟棄，不轉送出去給其它節點

M(*IP*)：這個 *IP* 被邀請的群播位址

CIP：某個指定的 IP

NS(IP_X, MAC_X)：傳送一個 NS 的封包，內容爲 *NS:* IP_X multicast to M(CIP) "Who has CIP" SLLA: MAC_X

DAD(IP_X, MAC_X)：傳送一個 DAD 的封包，內容爲 NS: [::](MAC_X) multicast to M(IP_X) "Who has IP_X "

NA(IP_X, MAC_X)：傳送一個 NA 的封包，內容爲 NA: IP_X unicast to CIP "I have IP_X " TLLA: MAC_X

非路由相關之威脅主要是以僞造 NS 或 NA 封包進行攻擊，我們系統利用追蹤重複位址偵測機制，記錄 IP 與 MAC 的對映關係以及其是否可以通行的狀態，因此攻擊者若要傳送僞造的 NS 或 NA 封包，企圖攻擊已經通過已取得系統通行權的 IP 位址，則 ND 防禦系統必定會發現攻擊行爲並且將其丟棄。如圖 10 所示，Station A 要設定新的位址 IP_A 時，會傳送重複位址偵測此 IP_A 是否有人使用，ND 防禦模組收到 DAD(IP_A, MAC_A) 即會在 IPv6_Status 加入一筆 (IP_A, MAC_A, *DADTest*)，經過 1 秒後沒有收到任何合法的 NA 回應 DAD，即將 (IP_A, MAC_A, *DADTest*) 的狀態改爲 PASS，在此之後 Attacker C 想要傳送 NS 或 NA 封包，將 IP_A 對應的 MAC_A 改掉，就會被 ND 防禦模組給丟棄。

此外我們也檢視 DAD 的過程中遭受攻擊的可能性。如圖 11 所示，Station A 在傳送重複位址偵測訊息來偵測 IP_A 是否有人使用過程中，Attacker C 想要以 NA 進行重複位址偵測 DoS 攻擊，而傳送 NA(IP_A, MAC_C)，但因爲 (IP_A, MAC_C) 的對應不在許可通行之中，就會被 ND 防禦模組給丟棄，而不會對 Station A 造成影響。

路由相關之威脅主要是以僞造 RA 封包傳送假的路由組態資訊進行攻擊，當 AP 收到 RA 會以 Legal_RA 表進行

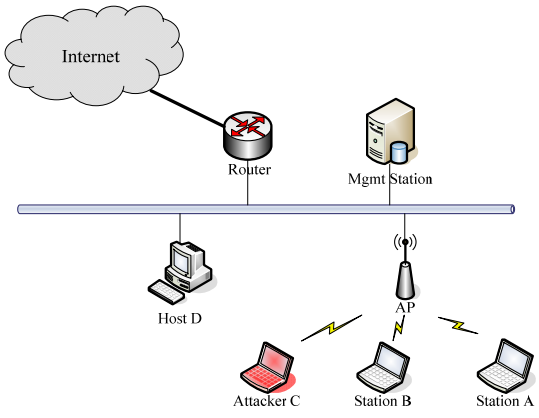

圖 9. 系統實驗環境

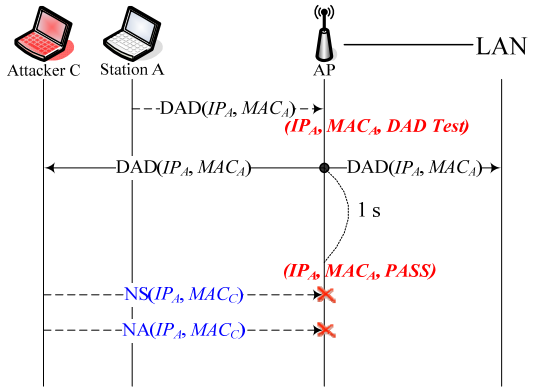

圖 10. 安全性評估（連結層位址重導攻擊）

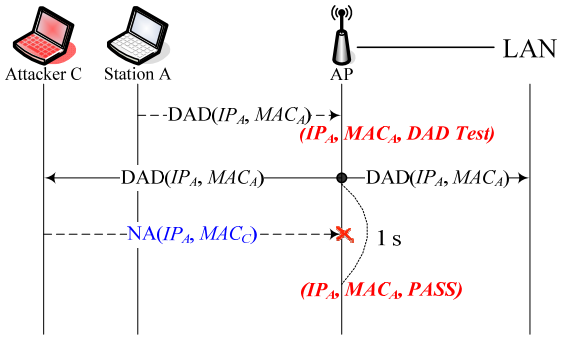

圖 11. 安全性評估（以 NA 進行重複位址偵測 DoS 攻擊）

比對將不合法的 RA 阻擋，所以攻擊者無法進行路由相關威脅的攻擊，如圖 12 所示。

經由實驗的結果，SEND 機制與本論文實作方法間各項目的差異，如表 4 所示。在位址碰撞機率的部份，因 SEND 產生 IPv6 位址的 Host ID 部份是以節點本身的公鑰及一些參數經由 SHA-1 雜湊函數產生，因此較一般 NDP 預設以 MAC 產生較不容易重複。

（二）效能測試

在效能測試方面，我們針對 NDP、SEND、AP+ND 防禦系統三種不同模式作效能比較。NDP 模式代表是一般情況下的模式，所有節點沒有任何 ND 保護的機制；SEND 模式代表在各節點安裝 Open Source SEND Project (send-0.2) 以提供 ND 安全機制；AP+ND 防禦系統模式代表在 AP 上建置 ND 防禦系統，其它節點以純 NDP 模式運作，系統會追蹤每個節點的 IP 狀態及阻擋偽造封包。其中在 SEND 與 AP+ND 防禦系統模式需另行安裝的軟體，如表 5 所示。在三種模式下，我們分別做了二種實驗，單純的 NS/NA 回應時間測量與在遭受攻擊的情況下 NS/NA 回應時間測量，來測量各模式對於處理芳鄰探索訊息及傳輸所需的時間。

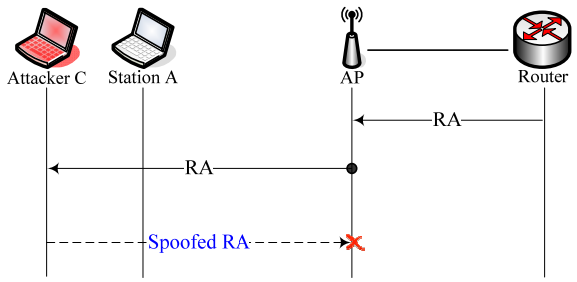

圖 12. 安全性評估（偽造 RA 攻擊）

表 4. SEND 與本論文方法比較

	SEND	本論文方法
位址碰撞機率	低	與 NDP 同
適用環境	任何環境	WLAN Infrastructure Mode
位址擁有權	CGA [8]	DAD
非路由相關之威脅	不會	不會
路由相關之威脅	不會	不會
額外負擔	每個節點需產生公鑰/私鑰 對於每個 ND 封包必需驗證	AP 上需過濾 ND 封包

表 5. NDP 模式外所需的軟體列表

節點	SEND 模式	AP+ND 防禦系統模式
Router	send-0.2	無
AP		ND 防禦系統
Station A		無
Station B		
Host D		

在實驗一中，我們測量由 Station A 以 ping6 產生 NS 傳送到 Host D，直到 Host D 回應 NA 給 Station A 所需要花的時間，測量 10 次在三種模式所得到的平均值如圖 13 所示。實驗結果顯示本文的方法只比一般的純 NDP 多了少許的時間，而 SEND 需要近乎 5 倍於 NDP 的時間。

在實驗二中，SEND 模式與 AP+ND 防禦系統模式，利用不同頻率的偽造 NS 封包攻擊，測量 10 次由 Station A 以 ping6 產生 NS 傳送到 Host D，直到 Host D 回應 NA 給 Station A 所需要花的平均時間。在 SEND 模式傳送的是偽造 SEND NS 封包，在 AP+ND 防禦系統模式傳送一般的偽造 NS 封包，所得到的實驗結果如圖 14 所示。

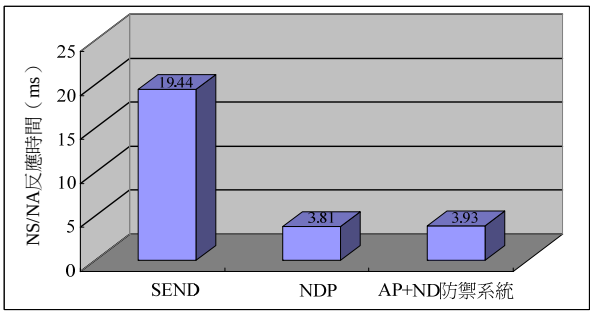

圖 13. 三種模式下實驗 NS/NA 回應時間

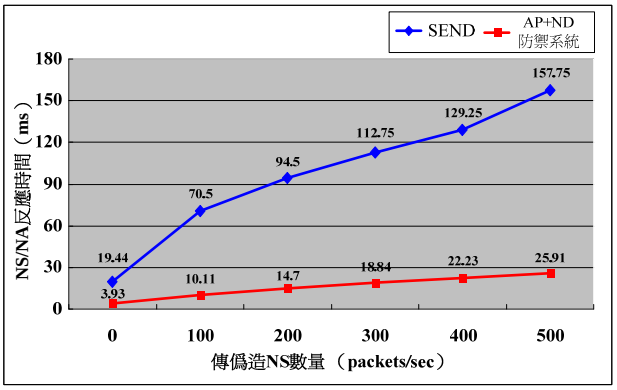

圖 14. 傳送偽造 NS 封包實驗 NS/NA 回應時間

因 SEND 模式在收到 SEND 的封包時需要驗證是否爲合法，當遇到大量僞造封包時就會更耗費時間，而我們的系統在 AP 收到封包時，僅需與 IPv6_Status 或 Legal_RA 表做比對，即可以阻擋僞造的封包，因此效能上比 SEND 要好。經由實驗可以證明本論文所提出的防禦系統足已抵擋芳鄰探索攻擊，且在效能上確實優於 SEND 的方法。

四、結論

目前以 IPv6 基礎的芳鄰探索協定，在無線網路下容易遭受攻擊。SEND 協定雖可保護芳鄰探索訊息不受僞造或竄改，但目前支援 SEND 協定的軟體甚少，且需在終端節點加裝 SEND 軟體，在驗證芳鄰探索訊息是否合法時，複雜的計算對於多數輕型的無線網路裝而言是一大考驗。本論文提出在 IPv6 無線網路下芳鄰探索安全威脅的解決方案，對於使用無線網路服務的使用者而言，在客戶端不需更動任何協定或加裝軟體。在此解決方案中，我們改良原有無線基地台，增加芳鄰探索的防禦模組與管理模組，直接阻擋僞造的芳鄰探索封包並將阻擋的記錄傳送給管理站。另外我們也對安全及效能作實測比較，結果證實我們系統是較 SEND 更有效率的，依本文的實驗數據來看，本防禦系統比 SEND 減少了大約 4/5 的處理時間。

參考文獻

1. Arkko, J., J. Kempf, B. Zill and P. Nikander (2005) *Secure Neighbor Discovery* (*SEND*). RFC 3971, Internet Engineering Task Force (IETF), Washington, D.C.
2. Arkko, J., T. Aura, J. Kempf, V. M. Mäntylä, P. Nikander and M. Roe (2002) Securing ipv6 neighbor and router discovery. Proceedings of the 3rd ACM workshop on Wireless security, Atlanta, GA.
3. Aura, T. (2005) *Cryptographically Generated Addresses* (*CGA*). RFC 3972, Internet Engineering Task Force (IETF), Washington, D.C.
4. Beck, F., T. Cholez, O. Festor and I. Chrisment (2007) Monitoring the neighbor discovery protocol. The Second International Workshop on IPv6 Today- Technology and Deployment- IPv6TD, Guadeloupe, French Caribbean.
5. Deering, S. and R. Hinden (1998) *Internet Protocol, Version 6* (*IPv6*) *Specification*. RFC 2460, Internet Engineering Task Force (IETF), Washington, D.C.
6. DoCoMo (2006) Open source SEND project. Retrieved March 18, 2007, available at http://www.docomolabs-usa.com.
7. Kent, S. and R. Atkinson (1998) *Security Architecture for the Internet Protocol.* RFC 2401, Internet Engineering Task Force (IETF), Washington, D.C.
8. Malinen, J. (2007) Host ap driver for intersil prism2/2.5/3, hostapd, and wpa supplicant. Retrieved May 20, 2007, available at http://hostap.epitest.fi/.
9. Narten, T., E. Nordmark and W. Simpson (1998) *Neighbor Discovery for IP Version 6* (*ipv6*). RFC 2461, Internet Engineering Task Force (IETF), Washington, D.C.
10. Nikander, P., J. Kempf and E. Nordmark (2004) *IPv6 Neighbor Discovery Trust Models and Threats.* RFC 3756, Internet Engineering Task Force (IETF), Washington, D.C.
11. Thomson, S. and T. Narten (1998) *IPv6 Stateless Address Autoconfiguration.* RFC 2462, Internet Engineering Task Force (IETF), Washington, D.C.

收件：98.01.07　修正：98.02.10　接受：98.06.01