增強行動隨意網路需求距離向量路由協定之安全性

Enhance the Security of AODV Routing Protocol for Mobile Ad Hoc Networks

張國清
義守大學資訊工程研究所
Email: cgc@isu.edu.tw

廖富民
義守大學資訊工程研究所
Email: freeball168@gmail.com

***摘要*—行動隨意網路 (mobile ad hoc networks)是一種暫時性網路，由許多行動節點所組成，行動節點之間可使用無線技術來互相通訊並具有容易佈建與低運作成本的特性，但是行動隨意網路因為無線電波的廣播特性與路由協定設計的缺陷，造成許多安全性的問題或漏洞，攻擊者可以利用這些漏洞來發動攻擊。本研究針對隨意網路之各種攻擊模式，透過使用時變數位簽章與雜湊鏈兩種機制來保護行動隨意網路需求距離向量(ad hoc on-demand distance vector, AODV) 路由協定之控制封包的安全。數位簽章用來驗證控制封包中固定不變之資料欄位，雜湊鏈則用來保護可變動的資料欄位，並於數位簽章的部分加入時變參數，避免簽章被惡意節點重複使用，至於在資料封包的保護方面，則於來源節點與目的節點收送控制封包時，相互交換時變參數，之後利用兩者的時變參數值導出一把溝通金鑰，並用此金鑰用來加密資料封包，以提高整體的安全性，本研究利用網路模擬器(NCTU-ns)來模擬所提出的方法，由模擬結果來探討其成效。**

***關鍵詞*—數位簽章 ; 雜湊鏈 ; 溝通金鑰**

***Abstract*— Mobile ad hoc network is an infrastructureless wireless network and is formed by a group of mobile wireless nodes which cooperatively communicate with each other using wireless technology. The features of ad-hoc networks are rapid deployment and low cost operation. Because of the broadcast nature of radio and secure weaknesses of the routing protocols, ad-hoc networks are usually susceptible to different security threats. In this study, we proposed a scheme to enhance the Ad-hoc On-Demand Distance Vector (AODV) routing protocol. We adopted two mechanisms to secure the AODV message. One mechanism used digital signatures to protect the non-mutable fields of the messages, and another mechanism applied hash chains to secure the only mutable information in the messages (hop count information). Besides, we added a seed value to digital signature to prevent that malicious nodes reuse the same digital signature, and in order to protect the data packets to be transmitted, source node and destination node must exchange each other's seed and then use these two seeds to derive a session key, which is to be used to encrypt and decrypt data packet. The performance of the proposed security mechanisms was evaluated by using NCTU-ns network simulator.**

***Keyword*—signature ; hash chains ; session key**

一、概論

行動隨意網路 (mobile ad hoc networks)其通訊環境為802.11，並可自我動態組織並讓行動節點彼此之間能在無基礎架構的情況下，即可隨時建立並經由無線的技術來互相通訊，因此，具有相當大的便利性與機動性。

行動隨意網路的建立、運作、維護都是透過其組成的無線節點。在行動隨意網路中，由於每一個節點的傳輸範圍有限，因此，兩個節點之間

通訊連結的建立，如果超出彼此的傳輸範圍，便需數個中間節點才能建立，也就是封包的傳送需透過鄰居節點的幫忙，所以任何一個節點在行動隨意網路中所扮演的角色(功能)，可為資料來源端(host) ，也可為路由器(router)，或兩者皆是，並與網路上其它節點共同進行網路的控制。當節點扮演路由器這個角色時，它的功能則為負責傳送封包到其他的節點，並可對經過它的封包做控管的動作，而做控管的動作則是為了避免那些被植入惡意程式碼的節點發動攻擊。

在行動隨意網路中，由於節點的數目眾多，要找出端點到端點間的路徑或者封包要如何被正確的傳送至目的節點，並不是一件容易的事情，所以需利用路由協定的使用。路由協定可區分為兩大類型，分別為預應式路由協定(proactive routing protocol)與反應式路由協定(on-demand routing protocol or reactive routing protocol)。

預應式路由協定的做法為每一個節點皆會維護一個完整的路由表，以便讓送出的封包能夠立刻得知到目的節點的路徑，維護的方式為路由表的更新，路由表的更新方式可為週期性更新與隨時更新兩類，此類型的協定優點為可讓每個送出的封包立刻得知到達目的地的路徑，不會有任何的延遲、路徑搜尋速度快、網路的穩定度佳，缺點為浪費無線網路的頻寬與節點的電源，此協定的代表有距離向量路由協定(distance vector routing protocol)、目的地序列距離向量路由協定(destination sequence distance vector routing) [1][2][3]。

反應式路由協定的做法為當欲傳送資料的節點有需要傳送封包時，才至網路上尋找相關的路由資訊，運作過程為來源節點向整個網路發送出一個路由詢問(route request，RREQ)，而繞徑狀態便在 RREQ 傳送過程中所經過的中間節點中建立起來，最後的目的節點會回傳一個路由回應(route reply，RREP)，來源節點收到回傳的 RREP 後，資料流便開始流通，此類型協定的優點為頻寬的使用量比預應式路由協定小、成本低、 控制封包比較不會增加網路負擔，缺點為封包平均延遲時間較長、路徑搜尋的速度較慢，此協定的代表有隨意網路需求距離向量(ad hoc on-demand distance vector, AODV)路由協定、動態來源路由協定(dynamic source routing)。

在這些路由協定中，AODV 是最常用於行動隨意網路的路由協定之一，然而 AODV 於設計之初，是假設每一個節點所在的環境是安全的，每一個節點都是可信賴的，所以並未將安全性列入考慮，但現實環境並非如此，因此攻擊者便利用 AODV 的安全性漏洞進行攻擊，有鑑於此，Pirzada and McDonald[4]、Ping Yi[5]、Zapata[6]等學者相繼提出一些方法，以升 AODV 的安全性。

Pirzada and McDonald[4]於 AODV 路由協定之上，另外加上群溝通金鑰(group session key)、金鑰交換協定(key exchange protocol)、溝通金鑰(session key)三個部分，以達到安全性需求，在所有路徑找尋的過程前，所有的節點必須與它周圍的鄰居確認一個群溝通金鑰，之後，節點發送 RREQ 封包出去前，將使用此群溝通金鑰加密後傳送，直到找到目的節點為止，RREP 的回應傳送方式則為 RREQ 方式的相反，路徑建立好後, 來源端與目的端再建立一把溝通金鑰，之後便可開始資料的傳輸，此金鑰主要的功用為保護資料封包。

Ping Yi 等學者[5]提出了一個抵抗洪氾攻擊(flooding attack)的方法，此方法主要是使用鄰居抑制(neighbor suppression)的方式來抵制 RREQ 洪氾攻擊,運作過程為, 首先節點會建立從它的鄰居節點送過來的 RREQ 的處理優先權與發送封包頻率的門檻值，由於節點剛開始都會設置發送封包頻率的門檻值，因此，如果一個原本發送 RREQ 的節點的頻率突然變高，且超出了節點所

設置的門檻值，那麼此節點的鄰居節點將不會再接收由此節點所發送的 RREQ，然後截斷(cutoff)攻擊者送資料封包過來的路徑，因此，透過此方式，攻擊者將無法執行 RREQ 洪氾攻擊。

Zapata[6] 在 secure-AODV (SAODV) 中假設，每一個節點擁有網路中所有節點的公開金鑰，若中間節點持有公開金鑰，便能驗證傳輸過程中所經過自己的繞徑封包，其運作方式為繞徑控制封包的發送者附加上它的 RSA 數位簽章(由來源端的私密金鑰所產生)和首位雜湊值(top hash)於繞徑封包中，當此封包於網路中移動時，中間節點將驗證其簽章和雜湊值，除此之外，中間節點還產生雜湊鏈的第 k 個元素(此處的 k 是代表所經過之節點的數目)，然後將其放入封包中，而 RREP 可由目的端節點直接回應，或者由中間節點要求目的端節點來回應。SAODV 透過延伸 AODV 欄位與公開金鑰驗證機制，提供 AODV 路由協定安全性的延伸，然而其安全性仍然有需要改進之處，對防禦方面來說，SAODV 除了可抵制修改與偽造式的攻擊，對於蟲洞(worm-hole)攻擊、路由表溢載(routing table overflow)、黑洞攻擊(black-hole attack)與 DoS 等攻擊並無法防禦。

本研究針對隨意網路之各種攻擊模式，增強 SAODV 路由協定，透過使用時變數位簽章與雜湊鏈兩種機制來保護隨意網路需求距離向量路由協定之控制封包，在資料封包的保護方面，則於來源節點與目的節點收送控制封包時，相互交換時變參數，之後利用兩者的時變參數值導出一把溝通金鑰，並用此金鑰用來加密資料封包，以提升整個行動隨意網路的安全性。

二、方法

(一) AODV 路由協定

AODV是以動態來源路由協定[7]與目的地序列距離向量路由協定[8]為基礎發展而來，整體架構分別採用DSR的基礎路徑建立、維護機制與DSDV 的逐跳路由(hop-to-hop) 與序列號碼(sequence number)為基礎。

在AODV路由協定中，除了一般的資料封包外，AODV還定義了繞徑所需的封包型態，稱為控制封包，並將此類封包分為四大類，分別為路由詢問(RREQ)、路由回應(RREP) 、限制型路由回應(Limited RREP)、路由錯誤(RERR)。

整個AODV的運作皆是建構於此四類封包，而於封包傳輸方面，所有封包的傳輸皆使用UDP/IP協定，並使用阜號654與網際網路位址(IP address) 255.255.255.255來對整個網路廣播封包。當網路於起始階段，來源端想要傳送資料封包給目的端，但不知路徑時，來源節點將檢查路由表中有無相關的路徑資訊可到達目的端節點，若有相關路徑資訊可到達目的端節點，則直接傳送資料封包；若無相關路徑資訊可到達目的端節點或路徑資訊已過期而被註記為無效時，便廣播RREQ給所有的鄰近節點，以搜尋能夠到達該目的節點之新路徑，如圖1所示。

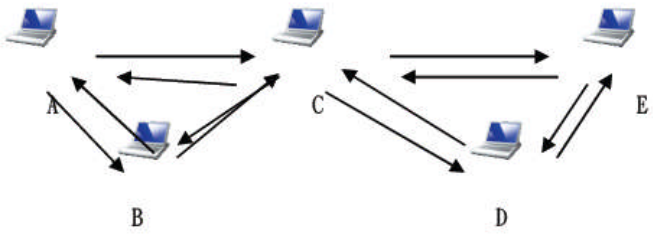

圖1 節點A找尋至目的節點E的路徑，以廣播方式傳送RREQ封包，實線箭頭為RREQ封包傳送路徑

當鄰近節點(或中間節點)收到RREQ封包之後，節點會做兩個動作，第一，先根據封包內之發起者IP位址、目的端IP位址與UDP/IP表頭的內容資訊搜尋本身路由表是否有到目的節點的相關路徑資訊，第二，檢查自己是否為RREQ封包所指定的目的端節點，若不是或沒有，就先依照RREQ封包的資訊紀錄修改自己的路由表，之後

再將所收到的RREQ封包廣播出去，並對發起此RREQ封包之發起者進行逆向路徑更新或建立，以利將來RREP封包的回送，反覆相同的動作一直到找到目的端節點或是找到相關路徑資訊為止。

當某個節點收到RREQ封包發現自己是RREQ所指定的目的端節點或是有相關路徑資訊可以到達目的端節點時，就先依照RREQ封包的資訊紀錄修改自己的路由表，再利用單播(Unicast)的方法送出路由RREP封包回到來源端節點，如圖2所示。同樣地，收到RREP封包之節點，也會建立或更新前往目的節點之路徑，以確保路徑資訊的最新狀態，途中所經過的節點再根據RREP封包內容所記錄的資訊去更改路由表，等回送的RREP封包被發起者收到後，來源端節點的路由表就含有到達目的端節點的資訊，並且一條具有雙向路徑資訊的通道就被建立完成，如圖3所示。

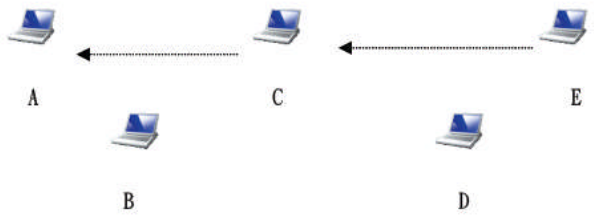

圖 2 節點 A 找尋至目的節點 E 的路徑，以單播方式回送 RREP 封包，虛線箭頭為 RREP 封包傳送路徑

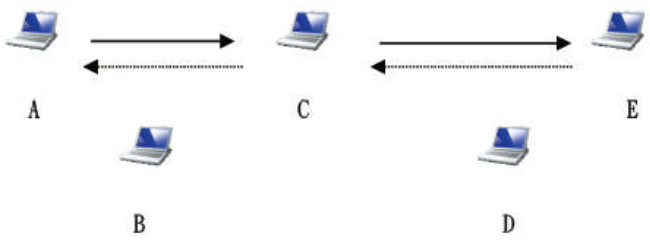

圖3 節點A找尋至目的節點E的路徑，雙向路徑資訊通道建立完成

若在路徑建立過程中，發起者接收到許多回送的RREP，則發起者將根據路徑選擇規則來建立到目的端節點的路徑。

來源節點與目的節點間雙向路徑建立完成後，並不代表所有工作都已結束，由於隨意網路是由行動節點所組成，而行動節點有可能因為電力不足、傳輸範圍有限、節點具移動性…等諸多原因，導致已建立好的路徑發生錯誤，因此便需透過路徑維護來保持通訊暢通，路徑維護的工作主要是透過發送RERR封包來達成。如果中間節點發現原路由之下一個節點(next hop)中斷，便發出路由錯誤封包通知其上游節點(upstream node)並嘗試區域性地恢復與目的節點的連結。

(二) SAODV 路由協定

SAODV 路由協定是架構於公開金鑰加解密(public key cryptography)的方式上，並使用數位簽章與雜湊鏈兩種機制來保護 AODV 封包的安全，數位簽章主要用來驗證固定不變之資料欄位，這可避免惡意節點偽裝為來源節點發佈路由詢問(RREQ)封包或偽裝為目的節點回覆路由回應(RREP)封包等攻擊並可保證資料的完整性與可靠性，雜湊鏈主要保護可變動的資料欄位，如控制封包的中繼節點數(hop count)，所以惡意節點在傳遞控制封包時，若修改中繼節點數將被識破，至於 SAODV 的運作過程將詳述如下。

在初始的階段，SAODV 假設每一個節點都有一對做數位簽章用的金鑰對(key pair)，這一對金鑰是由適合的非對稱加解密系統所獲得，除此之外，每個節點還必須擁有驗證資訊的能力，前置工作完備後，便開始整體的運作，首先，發送節點(sender)產生一個控制封包，這個控制封包送出前，需先使用節點本身的私密金鑰(private key)對這個封包做簽章，也就是加密不可變動的欄位，至於可變動的欄位(hop count)則使用雜湊鏈來加密，而這裡所提到使用雜湊鏈來加密的方式是重複使用 one way hash function 來達成，雜湊

鏈的詳細步驟與使用式子如下所敘述:

步驟 1: 於送出封包前，每一次節點將產生一個隨機亂數(seed)並將 max hop count 的值設為 IP 表頭內的 TTL (Time To Live)值，值給定後，便 hashing seed，hash 的次數為 max hop count 次，藉此便可得一數值，此一數值為 Top Hash。

Hash = seed

$Top\_Hash = h^{Max\_Hop\_Count}(seed)$

步驟 2: 當節點接收一個封包後，要繼續所有的後續動作前, 如重新廣播 RREQ 或向前遞送 RREP 封包之前，它必須先驗證所接收到的封包(驗證 hop count 值)，驗證方式如下:

$Top\_Hash == h^{Max\_Hop\_Count - Hop\_Count}(seed)$

Hash = h(Hash)

節點先對延伸欄位中的 Hash 值，也就是 seed，做 hop count 次 hash，後計算出 Top_Hash 值，藉此判斷 Top_Hash 是否相同，若相同則代表驗證成功。

節點做完數位簽章與使用雜湊鏈後便可將封包送出，之後，如果有節點收到此封包，那麼該節點必須先對此封包做驗證，驗證方式為使用發送節點的公開金鑰來驗證數位簽章，雜湊值的驗證為上一段所敘述(接收封包後)的驗證方式。

在整個 SAODV 的運作過程中, 比較值得注意的為數位簽章的部分，在 SAODV 中，數位簽章可分成單簽章(single signature)與雙簽章(double signature)，若使用單簽章，則為 SAODV 的基礎模式，在基礎模式中，中間節點若收到 RREQ 且本身具有到目的節點的路徑，中間節點無法對此 RREQ 回覆, 只有目的節點才有辦法對 RREQ 做回覆動作，因為 RREP 封包必須要使用目的節點的私密金鑰做簽章，如果使用雙簽章，來源節點產生 RREQ 封包時, 除了原本所產生的簽章外，它還會產生第二個簽章，第二個簽章是由來源節點虛構一個向它自己傳送的 RREP 封包計算而得，產生第二個簽章的目的是為了要使中間節點能夠針對來源節點所發出的 RREQ 封包做回覆的動作(如果中間節點有到目的節點的路徑)，因第二簽章產生後，中間節點便會將來源節點的第二簽章存放於自己的路由表中，等到再次接收到來源節點的 RREQ 封包, 如果本身有到目的節點的路徑，那中間節點便會使用已存的第二簽章產生 RREP 封包給來源節點。

(三) 增強 SAODV 的新路由協定(Enhanced SAODV, ESAODV)

ESAODV，整體可分成兩部分來探討，繞徑保護與資料封包保護，在繞徑保護方面，提出兩個方法，第一個方法為偵測惡意節點，其做法為在路徑找尋機制運作前發送具有不存在目的端 IP 位址的 RREQ 封包至網路中，若有收到回覆的 RREP 封包，代表網路中有黑洞的惡意節點存在，因為發動黑洞攻擊的惡意節點只要收到 RREQ 封包，便馬上回覆具有較小中繼節點數的 RREP 封包給發送 RREQ 封包的來源節點，藉此導引來源節點選取含有惡意節點的路徑，以此方法偵測網路中是否存有欲發動黑洞攻擊的惡意節點，若偵測出惡意節點，則將此節點的 IP 位址加入黑名單中，之後，於路徑找尋機制運作階段，網路中的任一節點，若收到由黑名單中的節點所送出的 RREP 封包，便將所收到的 RREP 封包丟棄，因此這種發送具有不存在目的端 IP 位址的 RREQ 封包至網路中的方式主要是利用黑洞攻擊的模式所採取的反制措施。第二個方法則改善 SAODV 的路由協定，在簽章的部分加入了隨機亂數(seed)，此法將導致每次送出的簽章值都不同, 所以就算惡意節點儲存了送出的其一簽章也無法達到攻擊的目的, 因此便能防禦黑洞攻擊，在資料封包保護方面，使用溝通金鑰來對資料部分加密，溝通金鑰產生的過程如下:

a. 來源節點送出 RREQ 控制封包前，先產生一個隨機亂數並用目的節點的公開金鑰加密此隨機亂數並放入 RREQ 封包的延伸欄位中，然後再送出控制封包。

b. 目的節點收到 RREQ 控制封包後，便使用本身的私密金鑰解出隨機亂數

c. 目的節點回應 RREP 控制封包前，先產生一個隨機亂數並用來源節點的公開金鑰加密此隨機亂數並放入 RREP 封包的延伸欄位中，然後再送出控制封包。

d. 來源節點收到 RREP 控制封包後，使用本身的私密金鑰解出隨機亂數。

e. 最後，來源節點與目的節點便利用彼此所送出及收到的隨機亂數值做 XOR 得到一把溝通金鑰，之後，便使用此金鑰對資料加密。

三、模擬實驗

由於無法實際於有數十台行動隨意網路的環境中實現所提出的方法，因此，在本論文中，將使用模擬軟體(NCTUns-4.0)[9][10]的方式來模擬所提出的方法。實驗所使用的平台為 Intel Core 2 Duo processor T7300 (2.0 GHz,800 MHz FSB,4 MB L2 cache)，記憶體為 3 GB DDR2。模擬軟體的模擬環境(如圖 4 所示)為:

a. 16 個節點分佈於 400x400 公尺的範圍中。

b. 16 個節點於 2400x2400 公尺的範圍中隨機移動。

c. 節點之間的間隔為 100 公尺。

d. 每個節點以 10m/s 的速度隨機移動。

e. 16 個節點中挑出兩個節點進行 UDP 連線，封包大小為 1000 位元組。

f. 16 個節點中挑出 0 至 2 個節點做為惡意節點。

g. 總模擬時間為 400 秒。

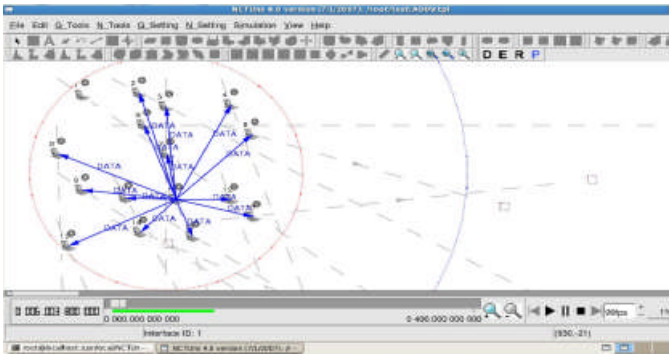

圖 4 模擬環境

在這個模擬環境中，將測試惡意節點數多寡對 AODV 與 ESAODV 效能的影響。

(一) 0 個惡意節點的 AODV 效能

首先，將先模擬 0 個惡意節點的情形，來源端節點為 1，目的端節點為 11，模擬完成後，得到如圖 5 及圖 6 的結果。

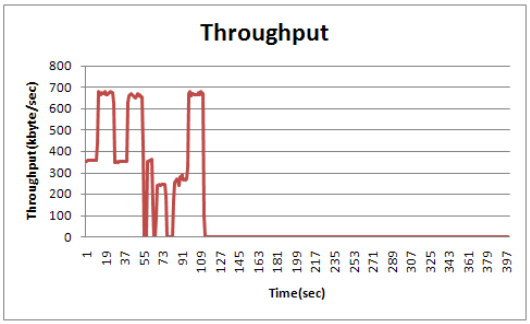

圖 5. 來源節點發送封包的總量

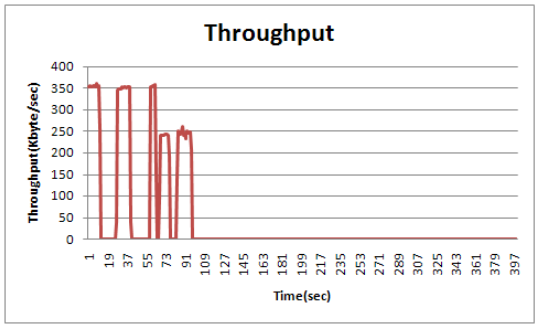

圖 6 目的節點接收封包的總量

由圖 5 及圖 6 可看出來源端節點與目的端節

點收送封包的總量曲線圖，在圖 6 中，由於原本建立的路徑中，有節點超出了彼此的通訊範圍，因此需重新找尋路徑，所以便產生目的端節點無收到封包的情形。

(二) 1 個惡意節點對 AODV 效能的影響

模擬 1 個惡意節點的情形，來源端節點為 1，目的端節點為 11，模擬完成後，得到如圖 7 及圖 8 的結果。

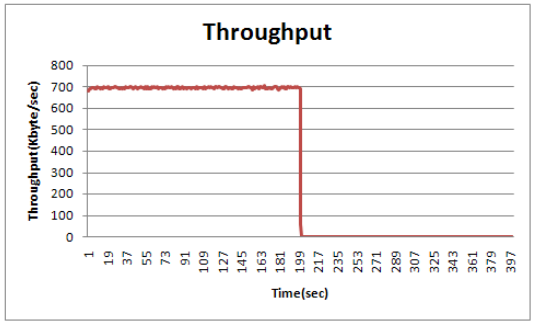

圖 7. 來源節點發送封包的總量

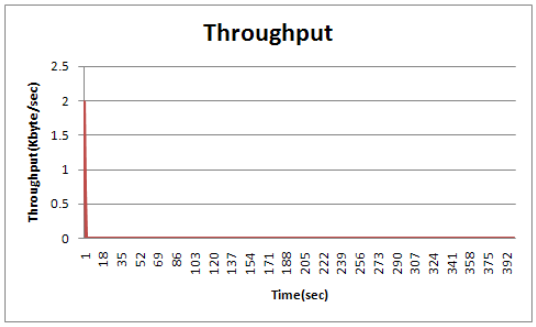

圖 8 目的節點接收封包的總量

由圖 7 及圖 8 可看出來源端節點與目的端節點收送封包的總量曲線圖，由於 AODV 繞徑協定於設計之初並未把安全性納入考量，因此，由圖中可發現，若環境中存在有 1 個惡意節點，AODV 繞徑協定便無法抵禦此惡意節點的攻擊，於是產生來源端節點送出的封包，目的端節點無法收到的情形，與無惡意節點的情形相比，1 個惡意節點便可對效能產生很大的影響。

(三) 2 個惡意節點對 AODV 效能的影響

模擬 2 個惡意節點的情形，來源端節點為 1，目的端節點為 11，模擬完成後，得到如圖 9 及圖 10 的結果。

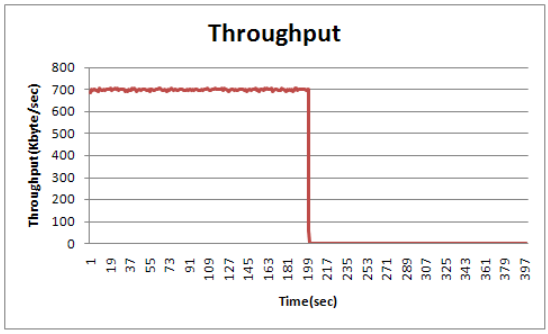

圖 9. 來源節點發送封包的總量

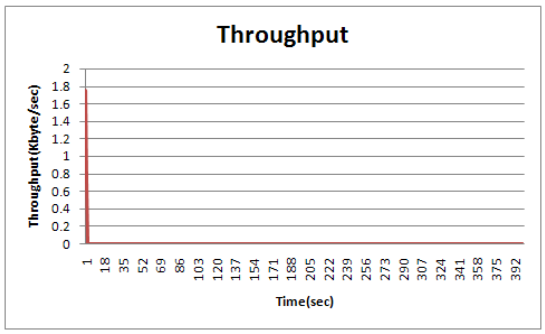

圖 10 目的節點接收封包的總量

由圖 9 及圖 10 可看出來源端節點與目的端節點收送封包的總量曲線圖，由於 1 個惡意節點便可產生很大的影響力，因此，由圖中可發現，若環境中存在有 2 個惡意節點，AODV 繞徑協定也無法抵禦 2 個惡意節點的攻擊，於是產生來源端節點送出的封包，目的端節點亦無法收到封包。

由上述的模擬與比較得知，若要使行動隨意網路能夠安全的通訊，必須要將 AODV 繞徑協定於設計之初未納入考量的安全性納入考慮，因此，我們所提出的方法便於 AODV 繞徑協定中加入安全機制，以提高行動隨意網路通訊的安全性。

(四) 0 個惡意節對 ESAODV 效能的影響

首先，將先模擬 0 個惡意節點的情形，來源端節點為 1，目的端節點為 11，模擬完成後，得

到如圖 11 及圖 12 的結果。

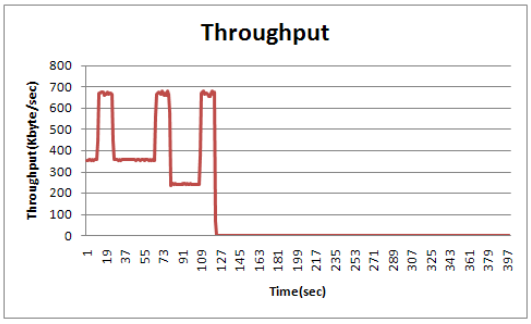

圖 11. 來源節點發送封包的總量

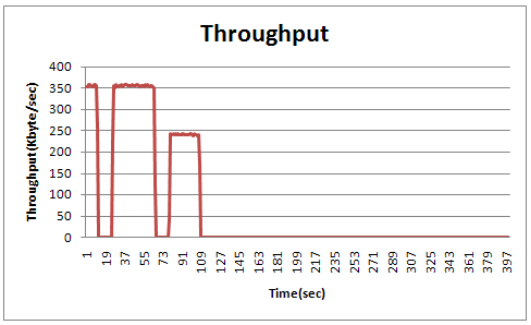

圖 12 目的節點接收封包的總量

由圖 11 及圖 12 可看出來源端節點與目的端節點收送封包的總量曲線圖，此部分與 AODV 相同，而在圖 12 中，也因為原本建立的路徑中，有節點超出了彼此的通訊範圍，因此需重新找尋路徑，所以便產生目的端節點無收到封包的情形。

(五) 1 個惡意節對 ESAODV 效能的影響

模擬 1 個惡意節點的情形，來源端節點為 1，目的端節點為 11，模擬完成後，得到如圖 13、圖 14 及圖 15 的結果。

在建立通訊路徑前，需先偵測網路中是否存在有惡意節點，圖 13 顯示出偵測出 1.0.1.8 為惡意節點，之後便將此節點加入黑名單中，爾後，若有節點收到此惡意節點的 RREQ 封包，便將之丟棄不處理，由圖 14 及圖 15 可看出來源端節點與目的端節點收送封包的總量曲線圖，由圖中可發現，若採用我們的方法，環境中存在有 1 個惡意節點，ESAODV 路由協定可成功抵禦此惡意節點的攻擊，於是來源端節點送出的封包，目的端節點依然可正常收到，與 AODV 繞徑協定相比，已大幅改善資料傳輸的安全性。

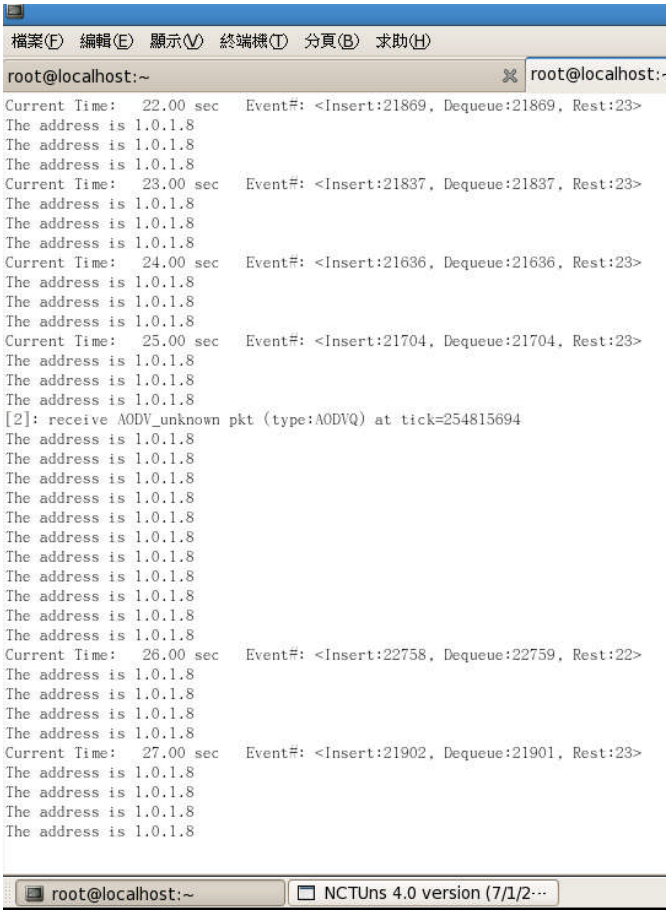

圖 13.偵測出 1 個惡意節點的模擬情況

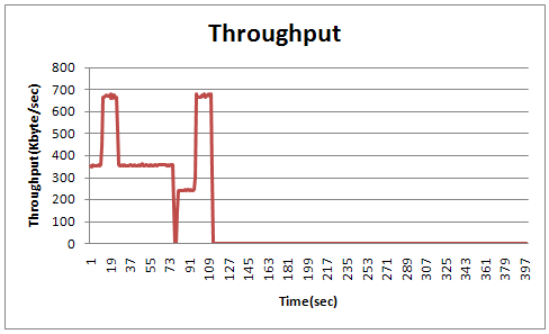

圖 14 來源節點發送封包的總量

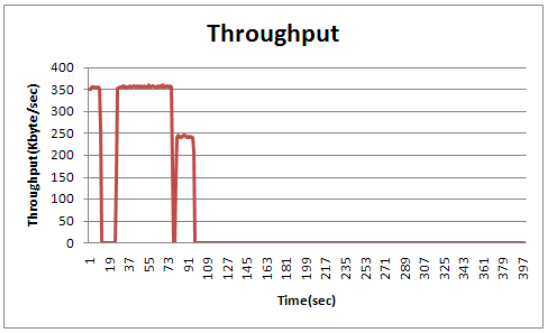

圖 15 目的節點接收封包的總量

(六) 2 個惡意節對 ESAODV 效能的影響

模擬 2 個惡意節點的情形，來源端節點為 1，目的端節點為 11，模擬完成後，得到如圖 16 及圖 17 及圖 18 的結果。

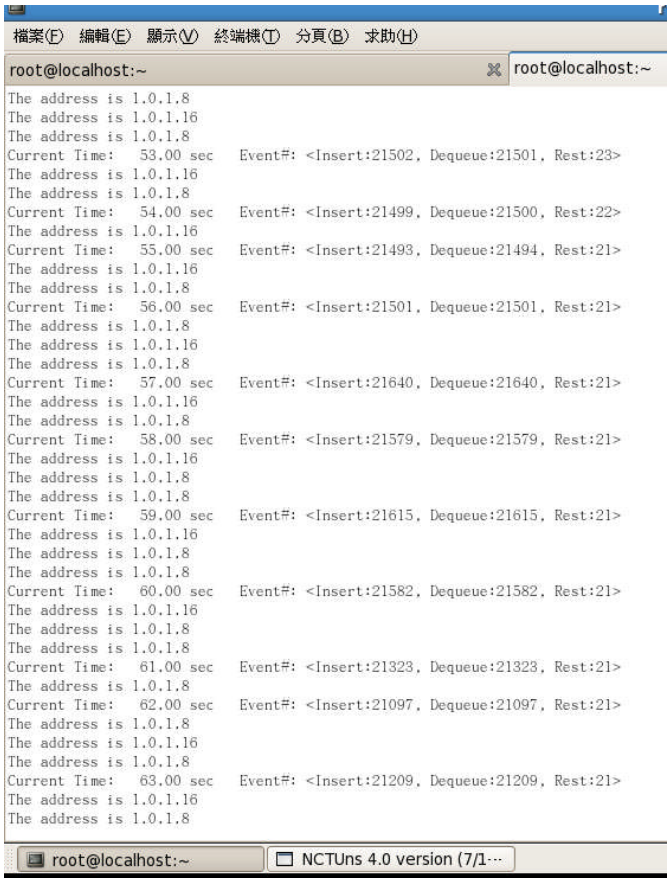

圖 16.偵測出 2 個惡意節點的模擬情況

在建立路徑前，依然需先偵測網路中是否存在有惡意節點，圖 16 顯示出偵測出 1.0.1.8 與 1.0.1.16 為惡意節點，之後便將節點加入黑名單中，爾後，若有節點收到惡意節點的 RREQ 封包，便將之丟棄不處理，由圖 17 及圖 18 可看出來源端節點與目的端節點收送封包的總量曲線圖，由圖中可發現，若採用 ESAODV，環境中存在有 2 個惡意節點，ESAODV 路由協定依然可成功抵禦此惡意節點的攻擊，於是來源端節點送出的封包，目的端節點依然可正常收到，圖 18 中，因為原本建立的路徑中，有節點超出了彼此的通訊範圍，因此需重新找尋路徑，所以便產生目的端節點無收到封包的情形，並非遭受惡意節點攻擊，由上述比較後，可發現，與 AODV 路由協定相比，已大幅改善資料傳輸的安全性。

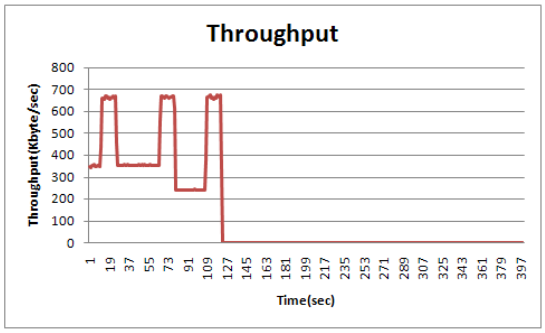

圖 17 來源節點發送封包的總量

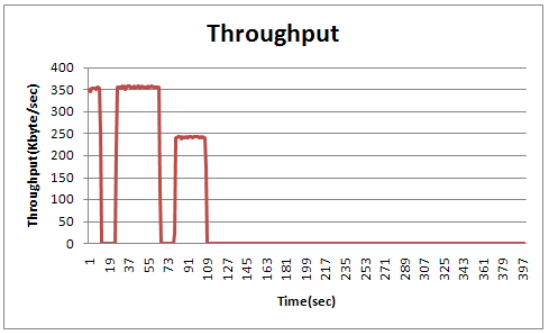

圖 18 目的節點接收封包的總量

四、結論

在本研究中，提出 ESAODV 路由協定，目的在於能夠於路徑找尋階段前有效偵測出網路中的惡意節點，並使惡意節點無法參與路徑建立過程，以確保之後所建立的路徑是一條安全無虞的路徑，並於數位簽章的部分加入時變參數，避免簽章被惡意節點重複使用，在資料封包的保護方面，則於來源節點與目的節點收送控制封包時，相互交換時變參數，之後利用兩者的時變參

數值導出一把溝通金鑰，並用此金鑰用來加密資料封包，以提高整體的安全性，在系統架構上，由於使用定期發送偵測網路中惡意節點的封包，可有效偵測出網路中的惡意節點，不過因為需要廣播許多的偵測封包，也會因此增加每個節點的工作量以及功率消耗，此外，為了實現我們所提出的方法且提高安全性，方法中只允許目的端節點能回覆 RREP 封包，因此，路徑找尋的時間將增加。

在研究行動隨意網路相關的攻擊以及防治已有相當多的論文相繼提出，但是沒有一個方法是完全沒有缺點，因此，如何改善其缺點，大幅度提高行動隨意網路通訊的安全性，將是我們未來努力的目標。

五、參考文獻

[1] 陳彥銘，林秉忠，“802.11 無線網路安全白皮書”，台灣電腦網路危機處理暨協調中心，民國 92 年。

[2] 陳昆陽,段裘慶，“Black-Hole Proof AODV routing protocol”，台北科 技大學電腦與通訊研究所，民國96年。

[3] 陳建民，“AD HOC 網路中監聽節點之偵測與反制”，銘傳大學資訊工程研究所，民國 95 年。

[4] Asad Amir Pirzada and Chris McDonald, “Secure Routing with the AODV Protocol”, Asia-Pacific Conference on Communications, Perth, Western Australia, pp. 57-61, 2005.

[5] Ping Yi, Zhoulin Dai, and Yiping Zhong, et.al, “Resisting flooding attacks in Ad Hoc networks”, In proceedings of International Conference on Information Technology: Coding and Computing, pp. 657-662, 2005.

[6] Manel Guerrero Zapata, “Secure Ad hoc On-Demand Distance Vector Routing”, Proceedings of Mobile Computing and Communications Review, Vol. 6, pp. 106-107, 2002.

[7] C.E. Perkins and P. Bhagwat, “Highly Dynamic Destination Sequenced Distance Vector Routing (DSDV) for Mobile Computers,” ACM SIGCOMM: Computer Communications Review, Vol. 24, No. 4, pp. 234-244, Oct. 1994.

[8] D.B. Johnson, D.A. Maltz and Y-C. Hu, “The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR)”, RFC 4728, February 2007.

[9] Shie-Yuan Wang, Chih-Liang Chou, and Chih-Che Lin, “The GUI User Manual for the NCTUns 4.0 Network Simulator and Emulator”, available at http://NSL.cs.nctu.edu.tw/nctuns.html.

[10] Shie-Yuan Wang, Chih-Liang Chou, and Chih-Che Lin, “The Protocol Developer Manual for the NCTUns 4.0 Network Simulator and Emulator”, available at http://NSL.cs.nctu.edu.tw/nctuns.html