在無線隨意網路上防禦黑洞攻擊之入侵偵測系統設計

蘇民揚[1,*]，江昆霖[2]，林俊淵[3]
[1,2]銘傳大學資訊工程學系
[3]銘傳大學資訊傳播工程學系
[1,*]minysu@mail.mcu.edu.tw

摘要

所謂黑洞(blackhole)是利用修改 sequence number 和 hop count 來強制取得路徑的一種攻擊方法。本研究是在 MANETs 網路上佈置適量的 IDS 節點，以偵測並防禦黑洞攻擊。IDS 節點必須設定在監聽模式 (sniffing mode) ，並執行一個稱為 ABM (Anti-Blackhole Mechanism)的機制，根據範圍內所監聽到的繞路訊息以偵測惡意節點，進而加以隔離。ABM 主要是根據一個節點的 RREQ 與 RREP 繞路訊息之接收與傳送間的異常來推算節點的可疑值，當可疑值超過門檻值，便廣播封鎖訊息給網路上的一般節點。本文使用 NS-2 印證所提之入侵防禦系統的效果，在適當門檻值設定下，IDS 節點可以在零誤報(no false positives)的情況下，快速封鎖惡意節點。

關鍵字：隨意式無線網路、AODV、惡意節點、黑洞攻擊、蟲洞攻擊、入侵偵測系統(IDS)

1. 緒論

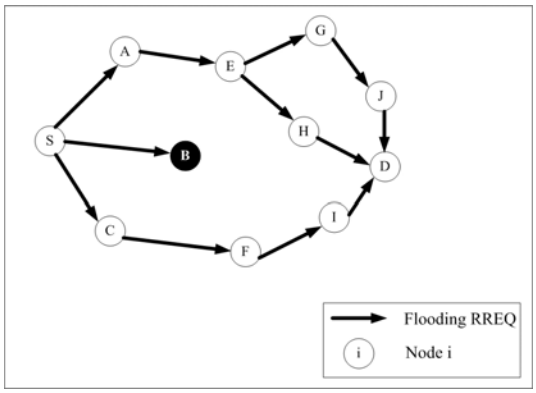
在無線隨意式網路中，由於它沒有像有線網路中的基礎存取點，是以多點跳躍(multi-hop)的方式來傳遞資料，每個行動節點不只是個端點，他們都還必須要扮演路由器的角色來控制協助繞路訊息。當來源節點(source node)想要傳遞資料給目的節點(destination node)時，必須透過兩端點間的中繼節點們(intermediate nodes)來幫忙傳遞訊息。因此要去建立一條穩定且快速的路徑，是 MANET 網路最重要的議題之一。無線網路的繞路協定有非常多的種類，主要分為主動式繞路協定(proactive routing protocols)與反應式繞路協定(reactive routing protocols)。

在主動式繞路協定中，兩個節點間的路徑在沒有需要傳送資料的情況下，節點還是會主動去找出通往該節點的路徑。每個節點通常會週期性地(period)更新繞路資訊，除此之外，當網路拓樸改變的時候，節點也會去更新繞路的資訊。這樣的更新動作可以確保目前繞路表(routing table)的訊息是最新而且最正確的。如 DSDV[1]、OLSR[2]即為主動式繞路協定。主動式繞路協定的路經更新速度快、路徑內容會比較正確。但是，在 MANET 網路中，每個節點大都是具有能源上和網路頻寬的限制，如果一直主動去發送繞路訊息，可能容易導致電力消耗過快。因此主動式的繞路協定會比較不適合使用於電力與頻寬…等，擁有資源限制的無線隨意式網路環境。所謂被動式繞路協定就是只有當兩個節點要傳遞資料時，才會去尋找路徑，建立路徑，又稱作 On-demand Routing Protocol。節點通常是用廣播的方式去作尋找路徑的請求(route request)來找到路徑。如 AODV[3]、DSR[4]等。

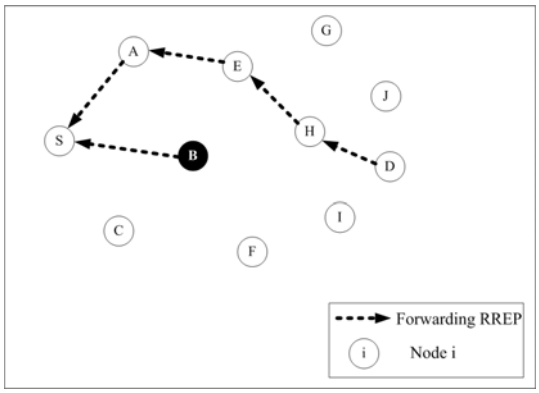
另外， MANET 網路常用於天災急救通訊、戰場通訊、商業會議等應用上面，當沒有所謂的基礎存取點的狀況下，要如何在兩端點間建立一條安全又可靠的傳輸路徑是個很重要的議題。在學術上及商業上有許多研究人員也開始著手研究提高安全性的無線繞路協定[5][6][7][8]，大部份安全繞路協定是針

對幾項安全威脅來做防禦，如基本的四項安全特性：(一)身分認證與不可否認性、(二)資源可利用性、(三)完整性、以及(四)機密與隱私性。黑洞攻擊主要針對修改繞路封包得到路權，進一步丟棄資料封包，主要威脅到上述安全性(二)(三)項。黑洞攻擊是個較為簡單且容易產生的一種攻擊行為，很容易普遍存在 MANETs 中。

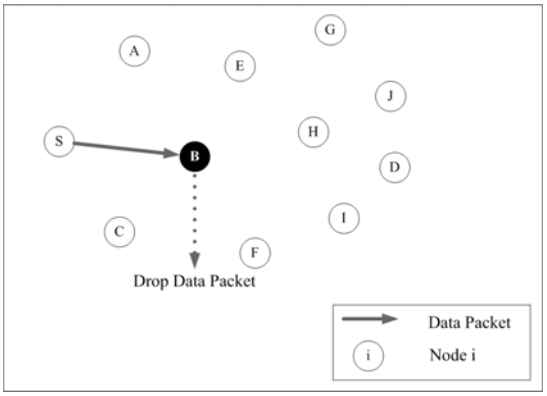
黑洞攻擊可以由單一節點完成攻擊或多個共謀完成攻擊。單一黑洞節點攻擊主要是修改繞路封包中用來判斷新舊封包的 Sequence Number 以及判斷路徑長短的 Hopcount，進而得到路徑，之後便將所有經過的資料封包丟棄。黑洞攻擊對於這類型使用 Sequence Number來判斷新舊以及用最短路徑取路的繞路演算法，例如AODV和DSR，會造成最為巨大的衝擊。例來源端S要去尋找目的端D，節點S會廣播RREQ封包去尋找目的節點D，正常的中繼節點收到後會將RREQ繼續廣播下去，而黑洞節點不會做繼續廣播的動作，如圖1(a)所示。當目的端D收到RREQ，會選擇一條hop count最小的路徑回傳RREP封包，而黑洞節點會直接回傳一個極大 Sequence Number以及hop count為1的RREP封包給來源端A，如圖1(b)所示。當來源端收到RREP封包會去選擇一條最新且最短的一條路徑，故選擇到黑洞節點傳送資料封包，而黑洞節點收到資料封包會直接做丟棄不處理，如圖1(c)。而多個惡意節點合作的黑洞攻擊型態，稱為Cooperative blackhole，主要特性如同於單一惡意節點，其不同處在於取到路徑後，當資料封包開始傳送至惡意節點B1時，B1會選擇性直接丟棄或者是傳送到惡意節點B2，由B2進行丟棄封包或監聽的動作，如圖1(d)所示，主要目的在於分散B1丟棄封包的比例，藉此可以減小被偵測程式發現的機率。



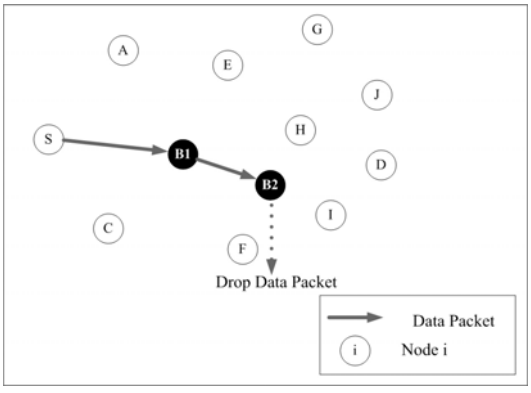
(a) RREQ flooding



(b) RREP replying



(c) Single blackhole attack



(d) Co-operative blackhole attack

圖 1 Blackhole 攻擊之圖示

[9]的作者Dokurer et al.提出，修改繞路協定去阻檔Blackhole取到路權，以AODV作為研究基礎，主要是來源端不接受回來的第一個RREP或是第二個RREP，而去處理接下來的RREP封包，目的是因為黑洞節點會迅速去回傳一個極大Sequence Number和Hopcount為1的RREP，所以這個研究可以有效防止黑洞節點位於來源端附近。在[10]中，Tamilselvan and Sankaranarayanan提出修改繞路協定使得來源端可以藉由安全通道去傳遞資料，利用等待和檢查每一個鄰居節點所傳送的RREP來決定一條安全的路徑。在中繼節點收到第一個 RREQ 後，它會將時間建立在'TimerExpiredTable'中，將'sequence number'和封包到達時間儲存到'Collect Route Reply Table' (CRRT)中，然後放入一個repeated next hop 傳送出去。到達目的端後，將會回傳RREP，當來源端收集到所有的RREP後，會去尋找CRRT 中可用的路徑，再對照是否存在有repeated next hop，選擇一條做安全路徑傳輸。

[11]中， Tamilselvan et al.提出一種可以防禦Co-blackhole的機制，稱為PCBHA。所謂Co-blackhole攻擊(B1、B2合作式Blackhole Attack)， 取路方式類似於傳統Blackhole攻擊，B1以快速回傳一個RREP的方式取路權，進而得到路權，然後來源端開始傳送資料封包給B1節點，當B1收到時，會選擇直接丟棄或是傳送到B2節點，而B2節點收到後會直接丟棄封包。而PCBHA機制，主要是在一個終止時間前，去收集所有的RREP中的資訊，存到一個 Table 中，叫 Response Collection table，而根據PCBHA演算法去選擇一條有效路徑。此演算法是會去根據一個AVG_FIDELITY_LEVEL，去判斷回傳之RREP是否大於一個 $\text{Threadhole}_{(in)}$ 和 $\text{Threadhole}_{(next\_hop)}$，藉此去尋找有效路徑。[12]中，Kurosawa et al.提出了一種利用動態訓練一段時間的傳遞封包來判斷的異常偵測機制，以特徵選取的方法來分析比對。此方法藉由收集發送RREQ的個數和收到RREP的個數，以及平均不同的Dst_Seq，首先會先訓練一組training data的規則，當新的資料進入節點，將會去比對然後判斷相似層度，若小於一個門檻值，則為正常行為，其他皆為異常行為，依此做為判斷。

本論文在網路拓樸上去佈置一些執行入侵偵測系統(Intrusion Detection System, IDS)的節點，它提供了判斷和隔離黑洞節點的機制。IDS 節點藉由 AODV 中的兩種繞路訊息(RREQ 和 RREP)的進出的模式來判斷範圍內是否有節點有異常的行為表現。由於偵測的主要工作由 IDS 節點負責，對於一般節點而言，不需負擔額外的計算工作，能有效的減少電力上的損失。

IDS 上所執行的防禦機制，稱為 Anti-Blackhole Mechanism (ABM)，用來監聽範圍內一般節點的繞路訊息，利用黑洞攻擊的特性，來觀察節點廣播 RREQ 以及回傳 RREP 時的異常行為，當異常值超過門檻值，會廣播封鎖訊息(block message)以隔離惡意節點。本論文後續編排如下，第二節會介紹 AODV 繞路協定的基本知識，以及幾篇有關黑洞攻擊的論文，第三節將詳細介紹本篇論文所提之方法，第四節是 ns-2 實驗數據與分析，最後第五節則是結論與未來展望。

2. 背景知識

AODV 擁有快速和可以動態做網路連結，使用 destination sequence numbers 的機制，可以讓同一個廣播訊息不會重複接收，避免在網路上產生無限迴圈。AODV 的路由訊息可分為路徑找尋(Route discovery)跟路徑維護(Route maintenance)這兩種。Route

Discovery 的部份可以分成以下兩種訊息：路徑請求(Route Request, RREQ)(圖 2(a))與路徑回覆(Route Reply, RREP)(圖 2(b)b)，而 Route Maintenance 可分為以下兩種訊息：路徑錯誤(route error, RERR)(圖 2(c))與 Hello message

Type	D	G	reserved	Hop count
RREQ ID				
Destination IP address				
Destination sequence number				
Originator IP address				
Originator sequence number				

(a) RREQ format

Type	A	reserved	Hop count
Destination IP address			
Destination sequence number			
Originator IP address			
Originator sequence number			

(b) RREP format

Type	reserved	Dest Count
Unreachable Destination IP address		
Unreachable Destination sequence number		

(c) RERR format

圖 2 AODV message formats

當source節點想要傳送資料給destination時，會有以下步驟：

1. source會先搜尋自己的Routing Table是否有到destination的路徑，這個部份分作兩個部份：a)如果有路徑的話，就檢查路徑是否過期，沒過期的話就依此路徑傳送資料封包出去。b)如果路徑過期或是Routing Table中沒有到destination的路徑，source端就會廣播RREQ封包給鄰居節點(one-hop以的節點)。
2. 當節點收到RREQ之後，就會先去檢查自己是否為此RREQ的目的節點，如果本身不是目的節點的話，此中繼節點會將RREQ欄位中的hop count值+1，並繼續廣播RREQ封包出去，直到目的節點收到RREQ封包才會終止廣播。
3. 如果接收端本身是RREQ的目的節點，那destination會先檢查是否收過此訊息，以及sequence number是否為最大值(最新的訊息)，之後destination會從眾多RREQ中挑選一條擁有最短hop_count的路徑。然候會依照RREQ傳播時所建立的反向路徑，並以unicast的方式回傳RREP封包給source端，目的節點之後會更新自己的Routing Table。
4. 在AODV協定中，會有著另一種情形，就是中繼節點會去回覆RREQ封包，即RREQ封包中的 ”destination-only flag”欄位要設成中繼節點也能回RREP封包，且中繼節點的路由表有到目的節點的最新路徑，這樣的情形，中繼節點就可以自己代替destination發出RREP給source端，達到減少網路上繞路訊息數量以節省網路頻寬。
5. 當source端收到RREP封包後，會先去更新自己的Routing Table，之後source就可以用此條路徑傳送資料封包給destination。

舉例如圖三所示，s與d分別代表來源節點與目的節點，灰色線條代表RREQ廣播過程，黑色線條代表中繼節點routing table中所存放的反向路徑，每個點只需知下一個節點為何，不需知道整條路徑所有節點的資訊。以g點而言，要回到s的下一個節點是f。以h點而言，它會收到來自e與g傳遞的RREQ，本例假設來自e的RREQ先到，故隨後來自g的相同RREQ就會被丟棄不予處理。圖三中只顯示routing table中的部份欄位。

假設沒有中繼節點知道到destination的路徑，當destination收到RREQ後，將以

unicast的方式回覆RREP至Source，如圖四。收到RREP的中繼節點，路由表內若無存在正向路徑(forward entry)，會先建立一個正向路徑並將RREP內值存入entry內對應欄位。若已存在正向路徑會比較該entry的destination sequence number以及RREP內的destination sequence number，如果後者較大，中繼節點將會根據RREP內容更新該entry內的值，之後再依照先前收到RREQ時建立至source的反向路徑，幫忙回傳RREP至source端。圖四中黃色為底的entry即為正向路徑，如此一來，source就能依照這條正向路徑，傳送資料封包給destination端。

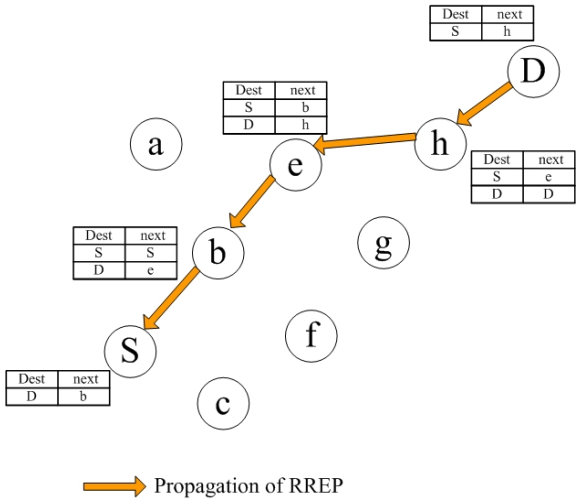


圖 4 RREP message of AODV

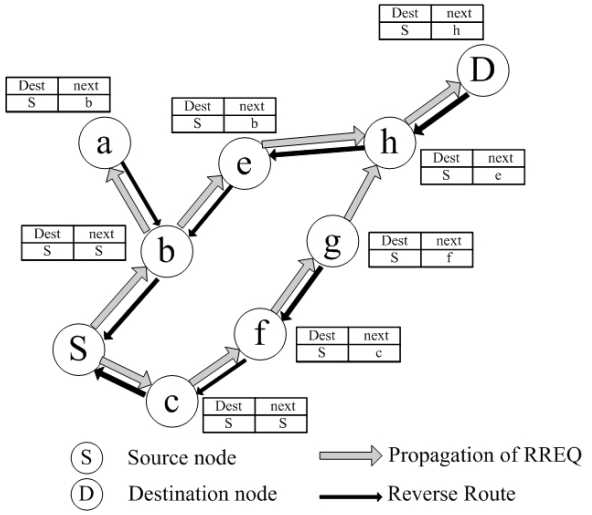


圖 3 RREQ message & reverse route of AODV

關於Route Maintenance的部份，每個節點都會週期性地發送Hello message，當鄰居節點在其傳輸範圍時會回覆此hello message，這樣節點就能了解有哪些鄰居節點在他的傳輸範圍內；所以當一段時間沒有收到鄰居節點的hello message時，他就能發覺有鄰居節點離開其傳輸範圍了，之後便會傳送RERR訊息給其Routing Table中有需求走此路徑的上游節點們，如圖五。當節點收到RERR封包後，會將損毀的路徑從Routing Table中刪除，以免下次又將資料封包傳往損毀的路徑，這樣就可以達成路徑維護的機制。

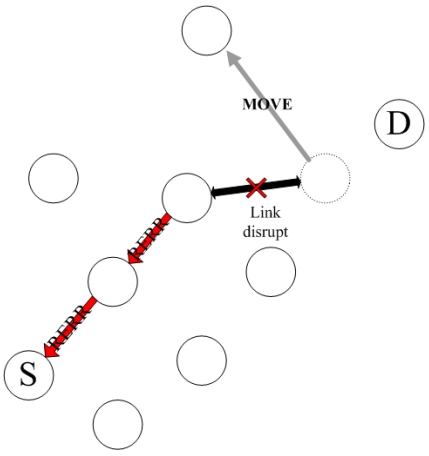


圖 5 RERR message of AODV

3. 研究方法

本篇論文提出一個機制，稱為ABM(Anti-Blackhole Mechanism)，來建立IDS節點，而我們些微修改AODV協定提供一般節點繞路使用。本論文提出在網路上去佈置IDS節點，可以節省一般節點在分析和判斷下電力上的浪費，也可以去抵禦蟲洞攻擊。本節利用在網路上佈署 IDS 節點的方式，去偵測並減緩 Blackhole 節點造成的傷害。本論文具有以下四點假設：

1. 網路上IDS的個數會依拓樸大小做增減。每個正常節點都至少會被涵蓋在一個IDS的傳輸/監聽範圍內。
2. 兩個鄰近的IDS節點會在對方的傳輸/監聽範圍內，以便可以彼此互相溝通。
3. 所有IDS節點擁有相同的一對public key/private key。
4. 每個IDS都被設定為錯亂模式，以監聽區域內的所有封包資訊。

在網路拓樸上，會有三類型節點，分別執行三種演算法。

1. 惡意節點：選擇性執行Blackhole AODV (BAODV)以進行黑洞攻擊。
2. 正常節點：執行些微修改之AODV (MAODV, modified AODV)以進行繞路。
3. IDS 節點：執行 ABM (Anti-blackhole Mechanism)演算法，以偵測並隔離惡意節點。

一般情況下，惡意節點表現有如正常結點。當攻擊發生時，惡意節點會改為執行BAODV，回應 RREQ 一個 sequence number 設為極大(如 4294967295)且 hop count 為 1 的RREP，以快速取得路權。當 BAODV 收到資料封包時，就會直接丟棄，不做任何的處理。

正常節點進入 MANET，會先廣播一個anonymous login message。鄰近IDS收到此anonymous login message，就會發送public key 給該節點，節點收到 IDS 的 Public key 後才可以做後續 AODV 之繞路動作。此後 IDS 發布訊息會用 private Key 簽署，而一般節點則用 IDS 的 public Key 驗證。IDS 偵測到有惡意行為時，會利用 block message 將最新的惡意節點 ID 廣播給範圍內其它所有節點。節點收到後，將最新的惡意節點新增到Block table，如表1。表1 表示節點目前收過 IDS_A 廣播的惡意節點 Node 1，及 IDS_B 廣播的惡意節點 Node 6，另外收到 block message 時間也會記錄在表中。IDS 廣播的block message 會用 private key 簽署，節點會使用 IDS 的 public key 驗證。所以，除了IDS 節點外，其他節點均無法廣播有效的block message。

表1 Block table

IDS node	Malicious Node	Time
IDS_A	1	2009/02/19 12:51
IDS_C	6	2009/02/19 12:55

MAODV 供一般正常節點繞路使用， MAODV 基本上與 AODV 相同，除設定不允許中繼節點回覆 RREP 之外，不同之處如下：1.增加了一個 Block table，用來記錄惡意節點名單。2. 節點收到 IDS 所廣播之 block message 時，會將 block message 中的惡意節點新增到 Block table 中。3. 節點在轉傳 RREP 封包時，若發現傳送 RREP 之節點存在 Block table 中，會丟棄不做處理。

本節以下將詳細說明 IDS 節點上所執行

之 ABM (Anti-blackhole mechanism)。ABM 使用兩個 Tables，稱之為 RQ Table 與 SN Table，分別如表 2a 與 2b。RQ Table 用來記錄 IDS 節點在監聽範圍內所看到的 RREQ 訊息，如表 2a 第一列表示針對(來源端,目地端,src_seq) = (1, 6, 3001)這個 RREQ，IDS 觀察到的節點 2, 4,及 5 廣播過且最大 hop count 為 2。SN (Suspicious Node) Table 則是 IDS 節點用來記錄監聽範圍內一般節點的異常值，如表 2b 第一列表示節點的異常值，主要是判斷是否為惡意節點的一個重要依據，例如節點 3 目前的異常值為 1，，尚未超過門檻值，故狀態為”inactive”，而節點 4 的異常值為 6，已達到門檻值，故狀態為”active”，實行封鎖。IDS 節點處理分為三個部份，說明如下。

表 2 RQ Table 與 SN Table

(a) RQ Table

Path			Hop count	Broadcasting nodes	Expired Time
Source	Destination	Src_seq			
1	6	3001	2	2, 4, 5	02:41:12
3	5	5012	4	1, 6	02:44:34

(b) SN Table

Node ID	Suspicious Value	Status
3	1	inactive
4	6	active

(A)IDS 監聽到 RREQ 時：以路徑的兩端點(i.e., RREQ 內來源端及目的端)及 source_sequence number 查詢 RQ table(表 2a)。若不存在此entry，則新增一個entry，將路徑兩端點，src_seq及hop count填入；並將廣播此RREQ節點的ID加入RQ Table中的「broadcasting nodes」欄位中，且「expired time」設定為current time + 15(s)。若存在此entry，將廣播此RREQ節點的ID加入「broadcasting nodes」欄位中，並判斷RREQ中的hop count是否大於該entry中的hop count值。若是，則將entry中的hop count值更新，然後將「expired time」加 3(s)；若否，則不處理。而系統會在一段時間根據 expired time 做清除 RQ Table 中過期的 entries。

(B)IDS 監聽到 RREP 時：判斷傳送 RREP 節點是否為目的端，若是，則不做處理。若不是，進入判斷 Blackhole 機制。先以 RREP 中的(來源端, 目的端,src_seq)為索引查詢 RQ Table。若 RQ Table 沒有對應的 entry (表示當初廣播 RREQ 時不在此 IDS 範圍中)，或 RQ Table 有對應的 entry 且「Broadcasting nodes」欄位有包含傳送 RREP 節點的 ID (表示合理的 RREP 回覆)，則結束不做後續處理。若 RQ Table 有對應的 entry 且「Broadcasting nodes」欄位不包含傳送 RREP 節點的 ID(表示不合理的 RREP 回覆)，再以傳送 RREP 之節點查詢 SN Table(表 2b)中”Node ID”欄，有下面兩種情形。Case 1:若存在此 entry，檢查狀態欄是否為 Active。若是 active，則結束不處理。否則，則將 SN Table 中該 entry 裡的 Suspicious Value 加 1，並判斷該 Value 是否超過門檻值。若超過門檻值，則將 Status 設為 Active，廣播 block message；若不超過門檻值，則結束不處理。Case 2:若不存在此 entry，則在 SN Table 中新增一個 entry，將傳送 RREP 節點 ID 填入，Suspicious Value 設為 1，Suspicious Status 設為 Inactive。

(C)IDS 與 IDS 之間的溝通：在(B)中，當 IDS 發現有新節點的異常值超過門檻值時，會廣播一個 block message 告知範圍內的其它節點，以便更新節點內的 Block Table(回顧表 1)。此時，根據假設條件 2，鄰近的 IDS 也會

聽到這個 block message。當一個 IDS 節點聽到鄰近 IDS 節點廣播 block message 時，做法如下。檢查 SN Table 之”Node ID”欄位，是否存在 block message 所發佈之惡意節點。如果存在且狀態欄為 inactive，則將狀態更改為 active，並廣播此 block message 以告知範圍內節點及鄰近 IDS；如果存在且狀態欄為 active(已廣播過 block message)，則丟棄不做處理。如果不存在，將 block message 中之惡意節點建立在 SN Table 中，Value 欄設定為門檻值，狀態欄設定為 active，並廣播此 block message 以告知範圍內節點及鄰近 IDS。

4. 實驗數據與分析

本論文利用NS-2 (Network Simulator Version 2)[13] 來作為我們用來實驗的模擬環境。本實驗我們使用兩種不同的方式分別去實驗黑洞攻擊。

4.1 單一黑洞節點

在 1000m x 1000m 的網路拓樸中，隨機分佈50個移動節點(使用MAODV)，固定一個黑洞節點(使用MAODV或BAODV)及固定的九個IDS節點 (使用ABM)，節點停留時間分別為0、5、10、15，節點移動速率：0~20 m/s，模擬時間為500秒。針對不同的pause time作十次實驗。選出20個移動節點做出10對連線進行每秒傳遞5kb的UDP CBR (Constant Bit Rate)資料連線，每個封包大小為512 bytes。如表3所示

表 3 實驗一參數

Simulated Area	1000X1000 (meters)
N=number of Nodes	60
Normal Node (AODV)	50
BlackHole Node	1(fixed)
IDS Node	9(fixed)
Simulated Time	500(s)
Mobility Model	Random Waypoint
Connections	20 (40 Nodes)
Traffic Type	UDP – CBR
Packet size	512 Bytes
Max Speed	20(m/s)
Average	20 times

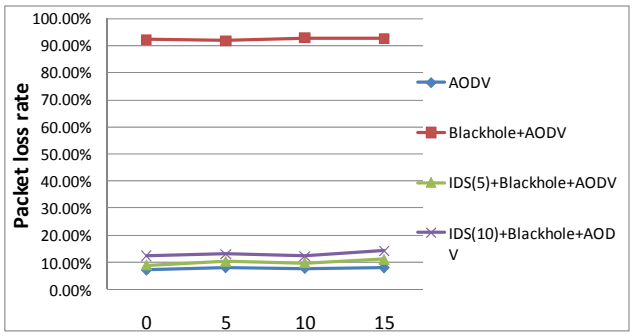


圖 6 Packet loss Rate

圖6表示在pause time不同的情況下，整個網路的封包遺失率，當有攻擊時而沒有IDS節點的時候，遺失率高達92%，而加入本論文中所提出的IDS節點，可以成功的降低到10%上下，而因為threshold不同，所遺失的數量也略不一樣。

圖7表示在pause time不同的情況下，整個黑洞節點所丟棄的封包佔總丟棄量的封包遺失率，當有攻擊時而沒有IDS節點的時候，遺失率高達48%~54%，而加入本論文中所提出的IDS節點，可以成功的降低到3%~5%上下，而因為threshold不同，所遺失的數量也略不一樣。

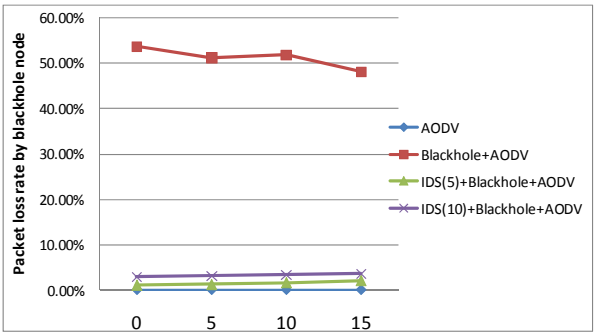


圖 7 Packet loss Rate by blackhole node

圖8表示在pause time不同的情況下，整個網路的Delay Time，當有攻擊時而沒有IDS節點的時候，Delay time會略長，而加入本論文中所提出的IDS節點，會使得Daley time稍微變小。

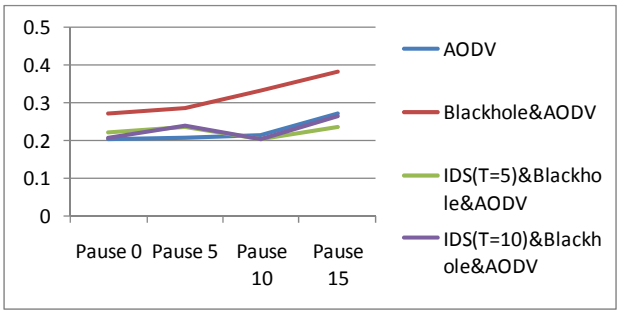


圖 8 Delay Time

4.2 多個黑洞節點

第二類實驗參數如下，在 1000m x 1000m 的網路拓樸中，隨機分佈50個移動節點(使用MAODV)，固定兩個黑洞節點(使用BAODV)，分佈在中央偏左下以及右下，以及固定的九個IDS節點（使用ABWM)。節點停留時間分別為0、5、10、15，節點移動速率：0~20 m/s，模擬時間為500秒。針對不同的pause time作十次實驗。選出20個移動節點做出10對連線進行每秒傳遞5kb的UDP CBR (Constant Bit Rate)資料連線，每個封包大小為512 bytes。如表5所示

表 5 實驗二實驗參數

Simulated Area	1000X 1000 (meters)
N=number of Nodes	61
Normal Node (AODV)	50
BlackHole Node	2(fixed)
IDS Node	9(fixed)
Simulated Time	500(s)
Mobility Model	Random Waypoint
Connections	20 (40 Nodes)
Traffic Type	UDP – CBR
Packet size	512 Bytes
Max Speed	20(m/s)
Average	20 times

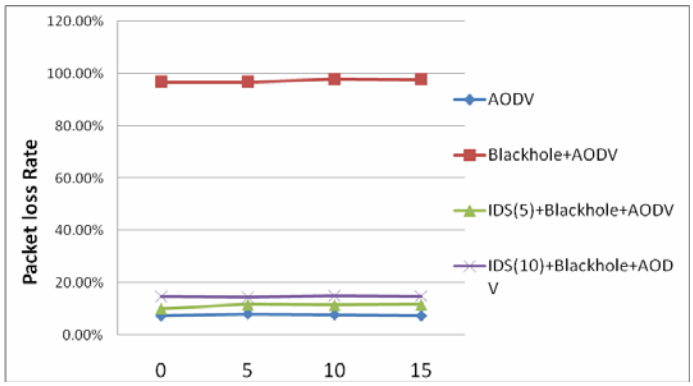


圖 9 Packet loss Rate

圖9表示在pause time不同的情況下，整個網路的封包遺失率，當有攻擊時而沒有IDS節點的時候，遺失率高達97%，而加入本論文中所提出的IDS節點，可以成功的降低到11%~18%上下，而因為threshold不同，所遺失的數量也略不一樣。

圖10表示在pause time不同的情況下，整個黑洞節點所丟棄的封包佔總丟棄量的封包遺失率，當有攻擊時而沒有IDS節點的時候，遺失率高達29%~36%，而加入本論文中所提出的IDS節點，可以成功的降低到2%~4%上下，而因為threshold不同，所遺失的數量也略不一樣。

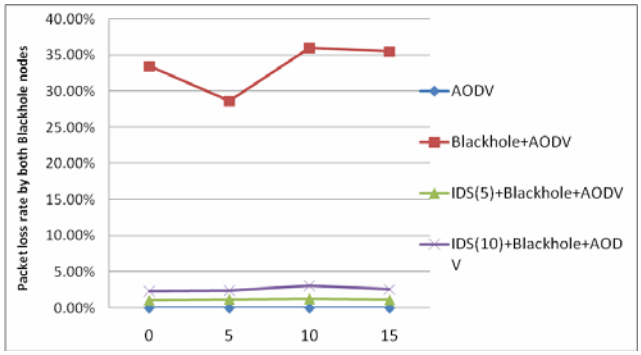


圖 10 Packet loss Rate by Both Blackhole nodes

圖11表示在pause time不同的情況下，整個網路的Delay Time，當有攻擊時而沒有IDS節點的時候，Delay time會略長，而加入本論文中所提出的IDS節點，會使得Daley time稍微變小。

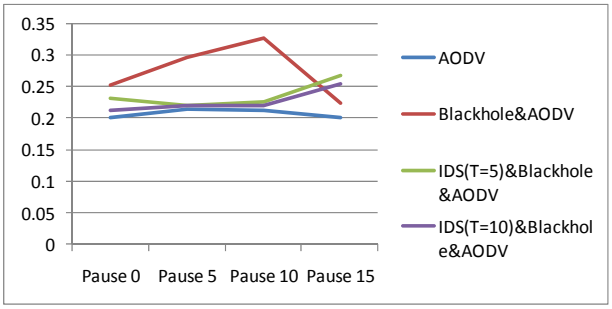


圖 11 Delay Time

5. 結論與未來發展

目前有許多研究致力於隨意式網路中的資訊安全系統，針對黑洞攻擊以及蟲洞攻擊的論文也是不少，但以分佈IDS節點作偵測引擎來防禦兩種類型的攻擊的相關論文比較少，本論文就是以這個出發點來防禦攻擊。本論文提出的ABM機制在實驗上可以確實的封鎖黑洞節點，使得網路上的封包遺失率可以從遭受攻擊時的92%降低到10%左右，百分之百的封鎖黑洞節點，並降低在網路拓樸上造成的傷害，不過相對的為了能有一條安全的路徑，會增加了些許封包在網路上的Delay時間。經由不斷地實驗可以發現，門檻值設定在5以上，False Positive 的值是非常的低，趨近於0的狀況。在未來可能會以不同的攻擊型態去作測試實驗，來嘗試本論文演算法在不同的型態攻擊是否可以成立，又是否能加以修改去封鎖更多不同類型的攻擊。

誌謝:感謝行政院國科會專題研究計畫之補助(97-2221-E-130-014, NSC98-2221-E-130-007)，使本論文得以順利完成。

參考文獻

[1] C. E. Perkins and P. Bhagwat, “Highly Dynamic Destination-Sequenced Distance-vector Routing (DSDV) for Mobile Computers,” *SIGCOMM*, UK, 1994.

[2] T. Clausen and P. Jacquet, eds, “Optimized Link State Routing Protocol (OLSR),” IETF RFC 3626, October 2003; http://www.ietf.org/rfc/rfc3626.txt.

[3] C. E. Perkins, E. M. Royer, and S. R. Das, ” Ad hoc on-demand distance vector (AODV) routing,” IETF INTERNET DRAFT, MANET working group, Jan. 2004. draft-perkins-manet-rfc3561bis-01.txt.

[4] D. B. Johnson, D.A. Maltz, and Y.-C. Hu, “The Dynamic Source Routing protocol for Mobile Ad-hoc Network (DSR),” *IETF Internet Draft* (*work in progress*), July 2004

[5] M.Zapata and N. Asokan, “Securing Ad-hoc Routing Protocols,” in Proc. Of ACM Workshop on Wireless Security (WiSe), Atlanta, GA, Sept. 2002.

[6] Kimaya Sanzgiri, Bridget Dahill, Brain Neil Levine, Clay Shields, and Elizabeth Belding-Royer, “A Secure Routing Protocol for

Ad hoc Networks." In Proceedings of the 10th IEEE international Conference on Network Protocols (ICNP'02), November 2002.

[7] Panagiotis Papadimitratos and Zygmunt J. Hass, "Secure Routing for Mobile Ad Hoc Networks," In *SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002)*, January 2002.

[8] Y.-C. Hu, A.Perrig, and Davic B. Johnson, "Ariadne: a Secure On-demand Routing Protocol for Ad Hoc Networks," in Proceedings of the ACM Conference on Mobile Computing and Networking (Mobicom), 2002, pp. 12-23.

[9] S. Dokurer, Y. M. Erten, and Can Erkin Acar, "Performance analysis of ad-hoc networks under black hole attacks," *in the IEEE proceedings of SoutheastCon*, pp. 148-153, 2007.

[10] L. Tamilselvan and Dr. V Sankaranarayanan, "Prevention of Blackhole Attack in MANET," The 2nd Int.l Conf. on Wireless Broadband and Ultra Wideband Communication, 2007.

[11] L. Tamilselvan and Dr. V Sankaranarayanan, "Prevention of Co-operative Black Hole Attack in MANET," *Journal of Networks*, Vol. 3, No. 5, pp. 13-20, 2008.

[12] S. Kurosawa, H. Nakayama, N. Kato, A. Jamalipour, and Y. Nemoto, "Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method," *International Journal of Network Security*, Vol.5, No.3, pp.338-346, 2007.

[13] The Network Simulator - ns-2, http://www.isi.edu/nsnam/ns/