TRAM: A Traceback Method using RAndom Moonwalks in AMI Meter Networks

徐詩淳[1] 徐雅琦[1] 徐彬海[2] 陳耀鑫[2] 鄭伯炤[1]
[1]中正大學通訊工程學系暨研究所
[2]工研院資訊與通訊研究所
{hisa918203;alicehsu00}@gmail.com, {becker;yaohsin}@itri.org.tw, bcheng@ccu.edu.tw

摘要

先進讀表基礎建設(Advanced Metering Infrastructure, AMI)是智慧型電力網路的一環，意指在家庭用戶的電表加上網路連線的功能，使得傳統人工抄表的工作得以自動化。其攸關用電計價，使之中安全議題變得分外重要，相應的網路行為鑑識能力是必須的。

由於智慧電表網路裝置之儲存空間與運算能力皆大幅受限，傳統的行為鑑識方法並不適用於此。TRAM 方法中，電表僅需關注週遭之流量訊息，並利用 AMI 運作中用電資訊週期匯整至集中器(Data Concentrator, DC)的機制轉移攻擊路徑重建之運算任務，藉此補足電表儲存空間小及計算能力欠佳的性質，並達到重建攻擊路徑的目的。模擬結果顯示 TRAM 在攻擊流量相對較大時，能夠達到較高的準確度。是為一個適用於 AMI 網路、輕量的追溯方法。

關鍵詞：
先進讀表基礎建設、智慧型電力網路、阻斷式服務攻擊、追溯、智慧電表

Abstract

AMI (Advanced Metering Infrastructure) is a vital component of the Smart Grid system, which adds family-use power meter with network wiring function and uploads the reading automatically instead of manual recordings. This project focuses on the design of the traceback mechanism in order to reconstruct the attack path where the attacker launches Denial of Service. With the lack of storage space and processing power on smart meters, the conventional traceback methods are not suitable in AMI. In our approach, each smart meter collects the traffic statistics in intervals on all interfaces, and Data Concentrator (DC) gathers the traffic information from all meters for reconstructing the attacking path if it needs. The simulation results show that the proposed approach is able to reconstruct the better attack graph than the Random Moonwalks method under various network scenarios (such as attack traffic volume, distance between the attacker and the victim, and normal traffic volume).

Keywords:
Advanced Metering Infrastructure, Smart Grid, Denial-of-service, Traceback, Smart Meter

1. 前言

近年，傳統的電力網路建設日漸老舊，也間接影響到供電的品質與效率，因此希望透過智慧型電力網路(Smart Grid, SG)**錯誤! 找不到參照來源。**的建置，達到供電的即時監視與自動化，並可蒐集資訊以分析用電供需。在智慧型電力網路的建置上，需先完成 AMI **錯誤! 找不到參照來源。**，即智慧電表的佈建，以此支援用電資訊監控之即時性與電力記帳之自動化。由於 AMI 牽涉到民生用電，除了要能即時準確的蒐集用電資訊，其上之安全議題也備受重視。對於網路中攻擊者所產生的攻擊行為，其應變依照攻擊階段可分為三種：預防、偵測以及攻擊行為結束後搜集相關證據與分析。要做到百分之百的攻擊預防實為困難，有鑒於此，在攻擊行為已然成為事實的狀況下，網路行為鑑識機制的存在更顯必要。

阻斷式服務攻擊(Denial of Service, DoS)是指攻擊者透過對頻寬的占用以及對裝置資源的消耗使被攻擊裝置無法對合法使用者提供服務。然而攻擊者在發起 DoS 攻擊時經常伴隨著冒名的行為，即是利用偽造之來源位址發送封包，使的以攻擊路徑重建方式追溯攻擊者位置變的不再直覺，因此，多種追溯方法便被研究者發表出來。

智慧電表網路有著儲存空間較小以及運算能力受限的問題，智慧電表網路由於和用電計算有關，其應用上更存在即時的因素。有鑒於智慧電表網路的特性，現有的針對阻斷式服務攻擊之攻擊路徑重建方法並不適用在這類型的網路之中。因此本研究提出適用於智慧電表網路的對阻斷式服務攻擊之攻擊路徑重建方法，以用於找尋蠕蟲的 Random Moonwalk **錯誤! 找不到參照來源。**方法為基礎，在其上加入流量概念。使其能在電表儲存空間有限與計算能力不足的限制下，利用電表流量資訊以重建攻擊路徑、追溯攻擊源頭。

本論文總共分成五個部分探討，在第一章說明研究目的與背景；第二章則對相關文獻做簡單介紹與比較；第三章將說明 TRAM 之架構與運作方式；於第四章以模擬結果呈現效能分析；最後第五章將

對論文做總結並提出未來展望。

2. 文獻探討

由於智慧電表網路資源有限的特性，DoS 這類攻擊常常伴隨著攻擊者的冒名行為，使追溯攻擊者的工作變得困難。許多藉攻擊路徑重建以達到對攻擊者之追溯目的之方法也相繼被提出。

SPIE (Short Path Isolation engine)[4]係由 Alex C. Snoeren 所提出。SPIE 利用資料產生引擎(Data Generation Agents, DGAs)、SPIE 集中處理引擎(SPIE Collection and Reductions, SCARs)以及 SPIE 追溯管理器(SPIE Traceback Manager, STM)架構出僅一個封包即可便能尋回攻擊路徑的方法。當封包經過路由器時，DGAs 會擷取特定長度的封包檔頭及內容輸入一系列的雜湊函數做運算**錯誤! 找不到參照來源。**，將運算結果與布隆過濾器**錯誤! 找不到參照來源。**中的所存放的陣列做比對以判斷是否儲存此封包的摘要，當入侵偵測系統(Intrusion Detection System, IDS)發現攻擊，便會告知 STM 關於封包、受害節點、攻擊發生時間等相關訊息，STM 驗證封包來源的可靠性後，便會詢問底下的 SCARs 以要求 DGAs 在特定時間所記錄的封包資料傳回，以利 SCAR 繪製其攻擊路線圖。SPIE 僅需得知單一攻擊封包的訊息便能進行追溯，相對的 SPIE 架構必須負擔額外的成本在部屬多個 SCAR 之上。此外，裝置必須對經過封包進行雜湊函數的運算並暫存，在運算能力與儲存空間上有較高的負擔。

機率封包標記(Probabilistic Packet Marking, PPM)係由 Savage **錯誤! 找不到參照來源。**等人所提出，其利用 DoS 係由攻擊者端發送大量封包予受害者之特性，藉由路由器機率性的對封包進行標記以達到攻擊路徑重建。PPM 在封包檔頭中新增了三個欄位做為標記之用，其分別為起始點、終點以及距離。當封包經過時，路由器將以事先給定之機率值(p)決定是否對此封包進行標記，倘若滿足機率值(p)，此時路由器便會將自己的 IP 位址填入起始點欄位，並在距離欄位填入 0。倘若不滿足機率值(p)，此時路由器將查看距離欄位是否為 0，若為 0，路由器將自己的 IP 位址填入終點欄位，並增加距離欄位值。若否，則路由器將不對封包有所作為。一個起始點、終點及距離資訊組合被稱為棱，由於 DoS 需利用到大量封包的發送，這些封包所經的路由器將有較大的機會對封包進行標記，也使受害者能蒐集到足夠的棱，將這些棱加以組合重建出攻擊路徑，以找出攻擊者所在位置。PPM 的做法不會對網路產生額外的負荷，也不會對路由器產生過大的負擔，並能夠做到在攻擊行為已完成情形下的事後鑑識。由於 PPM 需要網路裝置儲存大量的棱，並需要由受害者裝置自己進行演算，因此不適用在儲存空間受限、運算能力較小的智慧電表網路中。

連結測試**錯誤! 找不到參照來源。**的方法係由 H. Burch 等人所提出，以洪水控制來驗證通道情形。如其名，這個方法的觀念是下游節點發出大量的訊息量給上游節點，當節點發出訊息量後，會等待回傳的封包，並估量所回傳的訊息量。當回傳的訊息量相當於傳出去的訊息量，則判定此路徑為正常，並可以此方法由目的地端往來源端逐一縮減攻擊範圍，反之，當回傳的訊息量遺失了很多，則代表此路徑遭受到攻擊的可能性極大，使用這個方法的好處在於不用蒐集存放許多的封包資料，故不需要增加額外的儲存空間，但相對於其他的追蹤方式，其重建出的路徑精確度表現相對較低。最後，使用此方法會需要用到大量的頻寬，則會對網路造成更大的負擔，使網路壅塞的現象更為惡化，故此方法較不適用在智慧電表網路中。

Random Moonwalks **錯誤! 找不到參照來源。**係由 Xie 等人提出，利用隨機路徑選擇以找到攻擊者位置的方法。假設攻擊者位置位於整個流量圖樹狀結構之源頭，以隨機取樣的方式找出可能的攻擊路徑，以鎖定惡意流量之來源。由於此法不需要以龐大的資料庫來管理攻擊特徵，也不需要複雜的演算，若加以改良便能成為一個可應用在智慧電表網路的追溯方式，TRAM 方法便是以此法為基礎加以延伸。

與需要儲存封包摘要的 SPIE 以及較長傳輸路徑之上所有棱的 PPM 相較，連結測試、Random Moonwalks 以及 TRAM 對儲存空間的要求較少。此外，SPIE 必須對封包進行多個雜湊運算，其運算量會較其他方法來的多。連結測試對儲存空間與運算能力的要求雖然不高，卻只能在攻擊行為發生時進行追溯，不具有事後的行為鑑識能力。由於 PPM 僅在封包傳送時予以標記，並不會在重建攻擊途徑的過程中有更進一步的刪減。這點 SPIE 亦同。Random moonwalks 採隨機取樣的方式向上搜尋，只會在找到邊攻擊者，到達邊界亦或超出取樣時間時才會停止搜尋，故也沒有辦法縮減取樣基底。TRAM 方法以 Random Moonwalks 的方法為基礎，再利用流量與距離的資訊對取樣基底中的棱加以刪減，使追溯的範圍能被加以限制。上述各方法與特性之比較便如下表 1 所示。

表 1 追溯方法比較表

	SPIE [4]	PPM **錯誤! 找不到參照來源。**	Link Testing **錯誤! 找不到參照來源。**	Random Moon-walks **錯誤! 找不到參照來源。**	TRAM
Low Storage		X	X	X	X

need					
Low processing ability need		X	X	X	X
Post-forensic	X	X		X	X
Edge Elimination					X

3. TRAM

智慧電表網路環境可以想像成無線感測網路(WSN)的一種，在這類網路中的裝置因低成本之訴求，其電源、運算能力與儲存空間都大幅受限，也因此許多現有的攻擊路徑還原方法並不適用在此類網路。因此，為了在智慧電網環境中實現對攻擊路徑還原之機制，除了需要有效控制電表所使用的儲存空間，也必須將運算任務移轉至第三方來合作完成。

3.1 系統架構

為了在智慧電表網路中完成攻擊路徑重建工作，每個電表將記錄其與鄰點間以及其與其他遠端電表間的流量資訊。整個攻擊重建工作可以分為兩個部份,分別為資訊蒐集以及攻擊路徑重建。其中，資訊蒐集是由電表本身記載其與其他電表間的流量訊息為主，攻擊路徑重建之運算則交給集中器加以完成。

為了有效限制攻擊路徑還原所占用的儲存空間，在資訊蒐集階段，所有電表僅儲存與鄰點相關之流量資訊。此外，由於在 AMI 的運作過程中，集中器必須週期性自電表蒐集家庭用戶的相關用電資訊(週期通常為 15 分鐘)，集中器本身的運算能力與儲存空間並不像電表處處受限，在這裡可以將資料彙整以進行攻擊路徑重建的演算。

3.2 資訊蒐集(Information Collection)

在 TRAM 方法中的資料蒐集階段需要每個電表維護兩種流量資訊表，分別為鄰點流量資訊表以及連結流量資訊表兩種表格。

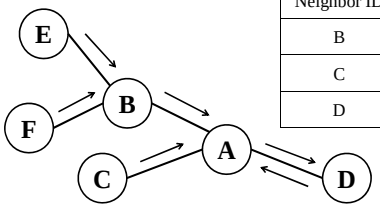
鄰點流量資訊表(Neighbor Flow Table)

鄰點流量資訊表則是紀錄來自電表週遭鄰點的封包數量，其格式如圖 1 所示。其中鄰點 ID(Neighbor ID)紀錄了該電表之鄰點電表的 ID 位址，計數(Count)為由此 ID 位址之電表流入該電表的封包數量。

Neighbor ID	Count

圖 1 鄰點流量資訊表

以圖 2 為例，其中封包的流量與方向以黑色箭頭表示。圖中可以看到電表 A 的鄰點流量資訊表，其上紀載了來自其鄰點電表 B、C 以及 D 的流量資訊。



Neighbor flow table on node A:

Neighbor ID	Count
B	240
C	112
D	50

圖 2 相鄰連結資訊表範例

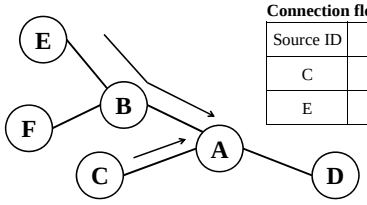
連結流量資訊表(Connection Flow Table)

連結流量資訊表格式如圖 3 所示，此表用以記錄與自身通訊之遠端電表的相關流量訊息，連結流量資訊表包含了三個欄位。其中，來源 ID(Source ID)記錄發起流量至該電表的來源電表 ID，計數(Count)記錄來源電表傳送給自身的封包數量，距離(Distance)為封包傳送至自身所需的距離。

Source ID	Count	Distance

圖 3 端點連結資訊表格式

以圖 4 為例，圖中展示的是電表 A 的連結流量資訊表，由此表可知電表 C 與電表 E 皆曾向電表 A 傳送封包，數量分別為 240 與 112。此外，由路由資訊中便能得知來自電表 C 與電表 E 的封包傳送至電表 A 所需距離。在此範例中兩者距離分別為 2 與 1。在這個例子裡，電表 B、D 及 F 皆未曾傳送連結封包給電表 A，在電表 A 的端點連結資訊表便不會有與電表 B、D 及 F 相關的資料列。



Connection flow table on node A:

Source ID	Count	Distance
C	240	1
E	112	2

圖 4 端點連結資訊表範例

為了得知封包傳送至自身的所需距離，利用已知的 TTL(Time To Live)最大值與封包到達目的電表時所剩餘之 TTL 數量，便能得到封包來源電表與接收端電表之間距離。距離之計算如下式所示。

$$Distance = TTL(Max) - TTL(packet)$$

智慧電表在資料蒐集階段之運作可參照下圖 5 之演算法。

```
Information collection procedure at node N:

Nt: Neighbor Flow Table(Neighbor, Count)
Ct: Connection Flow Table(Source, Count, Distance)

for each data packet P from node M{
   if(P. DestinationID == N){
      update Ct with the corresponding entry of M;
   }
   update Nt with the corresponding entry of M;
}
```

圖 5 資訊蒐集之演算法

3.3 攻擊路徑重建(Attack Path Reconstruction)

在 AMI 架構中，每隔 15 分鐘的週期，集中器便會自電表處蒐集家庭用戶之用電資訊，此時在資料蒐集階段所建立的兩張流量資訊表也能在集中器處做為整合，以利集中器做為攻擊路徑重建之用。

流量向量圖(Flow Vector Graph)

本研究利用資訊蒐集階段的鄰點流量資訊表建立出阻斷式服務攻擊之攻擊路徑所用的取樣基底。每個週期時間，集中器便能取得電表上儲存之流量資訊表。來自所有電表的鄰點流量資訊表經轉換為棱之後，所有棱便能夠組成一個流量向量圖(Flow Vector Graph, FVG)。

表 2 鄰點流向資訊整合

Meter ID	Neighbor ID	Count
V	M	350
	I	170
	D	160
B	A	200
C	B	180
D	C	160

Meter ID	Neighbor ID	Count
F	E	230
	J	50
G	F	180
H	G	170
I	H	170
L	J	300
	K	300
M	L	350

以表 2 所示，這裡整合了取自所有電表的鄰點流量資訊表，其中電表 ID 為鄰點流量資訊表之來源電表 ID。舉例來說，電表 ID 為 V 的電表其鄰點流量資訊表總共有 3 個項目，分別為來自鄰點 ID 為 M、I 以及 D 的電表。表 2 中的鄰點流量資訊表的項目轉換為棱，並將這些棱轉換為如圖 **6** 中的 FVG。

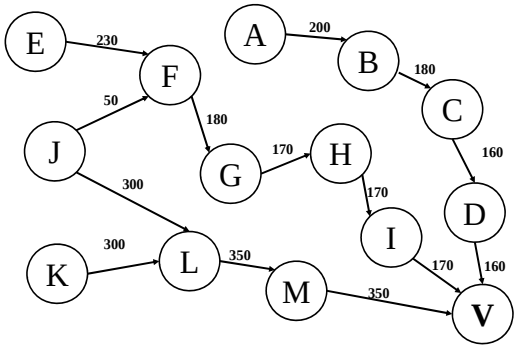


圖 6 流量向量圖(FVG)

有別於 Random Moonwalk 的 HCG，FVG 除了資訊的方向之外，也包含了流量的概念。這個 FVG 即為重建攻擊路徑時所使用的取樣基底。

棱刪減(Edge Elimination)

在利用 FVG 進行攻擊路徑重建之前，根據連結流量資訊表的內容，FVG 能夠再被精簡。

表 3 電表 V 之連結流量資訊表

Source ID	Count	Distance
X	150	4
A	200	4
K	300	3

延續圖 6 的例子，當 IDS 系統指出電表 V 中、來源 ID 為 X 的流量含有阻斷式服務攻擊，如表 3 所示，可以發現來源 ID 為 X 的項目中，其計數值為 150。此時將以 150 為基準，將 FVG 中流量小於 150 的棱刪除。此時，精簡後如圖 7 所示。

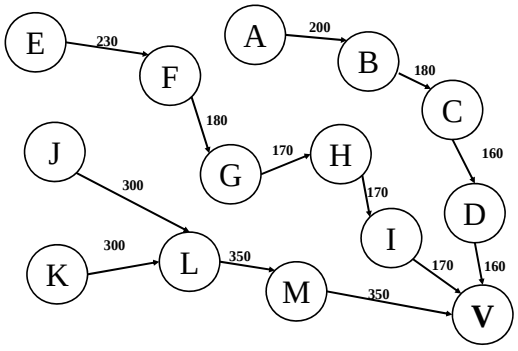


圖 7 棱刪減後的 FVG

在這個例子理，電表 J 與電表 F 間的棱因流量小於 150，因此從 FVG 刪除，以簡化攻擊路徑重建的過程。

距離限制(Distance Restriction)

延續圖 7 的結果，集中器會根據表 3 中、來源 ID 為 X 項目中的距離值，刪除距離不滿足的棱，在這個例子裡，以距離為 4 做為基準，距離不等於

4 的棱都會被刪除。

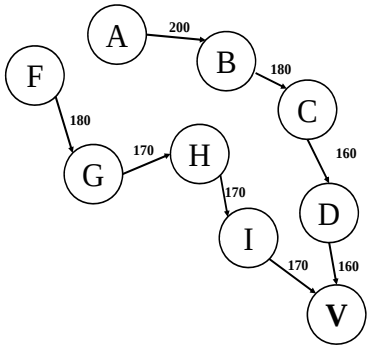


圖 8 簡化完畢之 FVG

經過棱刪減以及距離限制後得到精簡化的 FVG 如圖 8 所示，這個簡化完畢的 FVG 將會是攻擊路徑重建時取樣路徑所使用的基底。

隨機取樣(Random Sampling)

延續圖 8 的結果，以此 FVG 為基底，本研究與 Random Moonwalks 相同、採用隨機取樣的方式來重建攻擊路徑，在這個例子裡，可能被隨機取樣出來的路徑有 F → G → H → I → V 以及 A→ B → C → D → V 兩種，完成整個攻擊路徑重建的程序。

整個攻擊路徑重建之演算法如下圖 9 所示。

```
Path reconstruction procedure at DC for
victim node V:
//Nt: Neighbor Flow table(Neighbor, Count)
//Ct: Connection Tlow table(Source, Count, Distance)
//FVG: Flow Vector Graph
Let Path = The result of attack path reconstruction
Let A = the suspected source node;

Requests Ct, Nt from meters;
Produce FVG by Nt;

Edge elimination(FVG) base on A.Count;
Distance Restriction(FVG) base on A.Count;

Path = Random sampling(FVG)

Extract Path;
```

圖 9 攻擊路徑重建之演算法

4. 模擬及結果

在這節將以實驗模擬及其結果說明 TRAM 的特性。實驗環境與各項參數如表 4 所示。

本研究有幾項重要的假設：(1)在此網路環境中，攻擊者的攻擊路徑以及冒名的 ID 位址不會經常改變。(2)網路中並不存在共謀的情形。

表 4 實驗環境參數(資訊蒐集)

Parameter	Values
Simulation tool	Qualnet 5.0
Network topology	Grid
Simulation area	3 x 3 km^2
Number of nodes	10 x 10
Flow type	CBR
Simulation time	15 min
Routing protocol	AODV

TRAM 方法是以 Random Moonwalks 為基礎，路徑的交錯程度對路徑取樣的結果會大有影響，因此這裡也會利用增加正常流量之通訊對以觀察它們對攻擊路徑重建準確度的影響程度。每次實驗在攻擊路徑重建部分取樣 1 萬次，準確度即為取樣到正確路徑的比例。

此外，本文在 Random Moonwalks 方法的模擬上加入了距離限制的要素，在這裡以 Random Moonwalks-plus 表示之。

4.1 攻擊流量變化對準確度之影響

為了瞭解攻擊流量變化對攻擊路徑重建準確率的影響，這裡在網路中設置了 10 條起點不同、終點相同、起點與終點距離皆為 9 個節點之通訊對。其中 9 條通訊對之流量分別為 0.2, 0.3, … , 0.9, 1(封包/秒)，做為正常流量通訊對。另外一條通訊對做為攻擊流量之通訊對，這裡將觀察其流量由 0.1(封包/秒)以 0.1(封包/秒)為單位增加時，攻擊路徑重建的準確度變化。

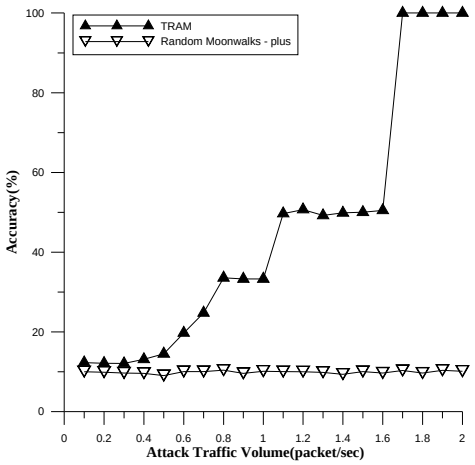


圖 10 攻擊流量對準確度之影響

圖 10 為攻擊流量對準確度之影響之模擬結果，由於 Random Moonwalks 並沒有流量概念，其攻擊路徑重建時的 FVG 取樣基底只會在一個定值上下震盪。TRAM 方法隨著攻擊流量上升，其 FVG 取樣基底縮減程度較高，其攻擊路徑的取樣選擇相對變少，準確度也因此變高。在 TRAM 的曲線中會呈現一種階梯的趨勢，這是由於並非每次攻擊流量的變化都能減少取樣的選擇，在同一個高度震盪的區間表示其 FVG 取樣基底中的取樣選擇數目相同。由此可知，隨著攻擊流量增加，TRAM 的表現也相

對較好。

4.2 攻擊者距離對準確度之影響

為了探討攻擊者所在與受害者之間的距離對準確度之影響,固定攻擊者產生的流量(1 封包/秒)，此時改變其所在位址使其與受害者位址間距離由 1, 3, …, 15, 17(hops)變化，以觀察距離變化對準確率之影響。在這裡，攻擊者距離指的是由攻擊者位址至受害者位址間所需要的最小跳躍數(hop)。

攻擊者距離對準確度之影響模擬結果如下圖 11 所示，可以發現攻擊者距離在 1 和 3 的時候由於距離較小，可以取樣的路徑組合也相對有限，因此準確率與距離在 5 的情形相比之下來的較大。當攻擊者距離持續增加，並超越所有的正常流量路徑的長度時，FVG 僅會存在攻擊者所使用的路徑，變成只存在唯一解的情形。

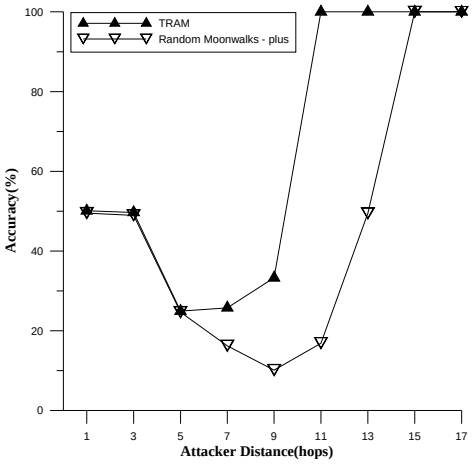


圖 11 攻擊者距離對準確度之影響

由於 TRAM 有依據流量刪減棱的機制存在，因此隨著攻擊者距離增加，其準確度的調升會比 Random Moonwalks 來的快，但當攻擊者距離超過了平均路徑長度的範圍時，TRAM 與 Random Moonwalks 的準確路將先後調升。

4.3 正常流量通訊對對準確度之影響

由於 TRAM 方法試圖利用觀察流量特徵來辨別攻擊者流量的可能傳遞路徑，因此在攻擊流量流經的路徑與正常流量交錯時較容易造成追溯源頭時的誤判。但由於多數 DoS 仰賴大量封包的發送來達到攻擊目的，因此以交錯的通訊對與其流量的調整來觀察對準確度的影響為何，此時將額外增加的正常流量通訊對數目固定在 5 條，並將這五條通訊對的流量由 0(封包/秒)依序增加至 1.1(封包/秒)，並觀察在不同的正常流量通訊對流量下，其對準確度之影響為何。

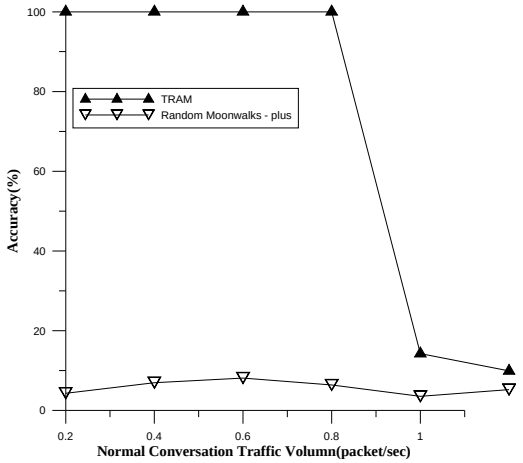


圖 12 正常流量通訊對流量對準確度之影響

模擬結果如圖 12 所示，在正常流量通訊對數目固定的情形下，倘若這些正常通訊對的流量較小，對 TRAM 而言準確度上並不會造成影響，Random Moonwalks 由於沒有流量觀念，其準確度之範圍隨著 FVG 的大小變化，但其 FVG 圖始終較會對其進行簡化的 TRAM 來的複雜。然而當正常流量持續增加,由於路徑重疊的關係,這些通訊對的流量在 1(封包/秒)左右便也開始對 TRAM 方法造成影響，這個影響在正常通訊對流量到達 1(封包/秒)以上時更為明顯，因為此時正常流量與攻擊流量的大小差異不大。

總結來說，由於 Random Moonwalks 不存在流量概念，一般情形下也沒有路徑距離的限制，在追溯的過程中，其準確度根據 FVG 的原始大小而隨意變換。TRAM 延伸了 Random Moonwalks 的概念，利用流量大小與距離限制進行棱刪減以簡化取樣基底，使 FVG 能被精簡。因此 TRAM 方法在攻擊者流量較大的情形下，能有較好的表現。

5. 結論及未來展望

TRAM 延伸 Random Moonwalks 的概念，使電表僅需儲存有限的流量資訊，並於每 15 分鐘的資訊蒐集時期將這些訊息集中至運算能力較大的集中器上進行攻擊路徑重建之演算，以滿足智慧電表網路儲存空間有限與運算能力不足之特性。

TRAM 尚有許多延伸的空間，在 FVG 的簡化上能夠導入其它資訊使其更加精簡，例如分類器的搭配。路徑取樣的部分也可導入相關資訊使每條路徑有不同的取樣權重，以提高路徑取樣的正確率。

參考文獻

[1] Luan Wenpeng, "Advanced metering infrastructure." Southern Power System Technology 3.2 (2009): 6-10

[2] Akash Singh, “Smart Grid Architecture.” Cancer Imaging, 2012

[3] Yinglian Xie, Vyas Sekar, David A. Maltz, Michael K. Reiter, Hui Zhang, “Worm Origin Identification Using Random Moonwalks.” IEEE Symposium on Security and Privacy 2005: 242-256

[4] Alex C. Snoeren, “Hash-based IP traceback.” SIGCOMM 2001: 3-14

[5] Nick G. Duffield, Matthias Grossglauser, “Trajectory sampling with unreliable reporting.” IEEE/ACM Trans. Netw. 16(1): 37-50 (2008)

[6] Burton H. Bloom, “Space/Time Trade-offs in Hash Coding with Allowable Errors.” Commun. ACM 13(7): 422-426 (1970)

[7] Stefan Savage, David Wetherall, Anna R. Karlin, Thomas E. Anderson, “Network support for IP traceback.” IEEE/ACM Trans. Netw. 9(3): 226-237 (2001)

[8] Hal Burch, Bill Cheswick, “Tracing Anonymous Packets to Their Approximate Source.” LISA 2000: 319-327