An Efficient Packet Marking Probabilistic Algorithm for Minimizing the Convergence Time in Wireless Sensor Networks

陳煥[1] 李宜靜[2] 廖國潭[3] 鄭伯炤[4]
[1,2,3,4]國立中正大學 通訊工程學系
{huan@ee.ccu.edu.tw; jean@insa.comm.ccu.edu.tw; g95430040@mail.comm.ccu.edu.tw; bcheng@ccu.edu.tw}

摘要

無線感測網路(Wireless Sensor Network －WSN)包含許多具有感測、運算和無線通訊能力的感測器，它可以用來偵測週遭的環境,且能應用在許多領域，不過 WSN 卻存在一個很大的缺點－資源有限。當攻擊者發動分散式阻斷式攻擊(Denial of Service－DoS)，攻擊者會傳送大量封包到受害主機，此舉會影響在攻擊路徑上的節點使其消耗資源，更甚者造成網路癱瘓。在傳統 IP 網路中，Edge Sampling 是很有名的方法對於追蹤阻斷式攻擊或分散式阻斷式攻擊 (Distributed DoS－DDoS)攻擊，不過由於重建攻擊路徑需要大量的封包，換句話說，會消耗很多的能量。本篇論文著重於如何減少重建攻擊路徑所需的封包即降低其收斂時間。所以本篇論文提出一個適合 Hieratical WSN 方法－Hierarchical Probabilistic Dice Function (H-PDF)，不只可以降低 Edge Sampling 的收斂時間，並可以改善 Edge Sampling 只能偵測一個攻擊者之缺點。經由模擬實驗證實 H-PDF 在 Hieratical 架構上，具有優異的收斂時間之性能。

關鍵詞：DoS, WSN, Packet Probabilistic Marking, Traceback, Convergence Time

Abstract

Wireless Sensor Networks (WSNs) contain a great number of nodes with sensing, computation, and wireless communications capabilities. WSN technology is ubiquitous to monitor and control environments in a variety of applications. However, WSNs have a grave threat – resource constraints. A DoS/DDoS attack may result in network disasters due to the energy exhaustion of the nodes along the attacking path. Edge sampling is a well-known traceback solution for DDoS attacks in traditional wired network, but it requires large number of packets to reconstruct the attack path. In this paper, we introduce an equality approach, called the Hierarchical Probabilistic Dice Function (H-PDF) suitable for hierarchical WSN, which enables edge sampling algorithm to reconstruct attacking paths with fewer collected packets under multiple attacks. The effectiveness of the proposed scheme has been demonstrated in our simulate studies of convergence time that have successfully used this H-PDF approach in hierarchical wireless sensor network environment.

Keywords：DoS, WSN, Packet Probabilistic Marking, Traceback, Convergence Time

1. 前言

科技日新月異，以往只能依賴人工的工作，現在都被許多科技所取代，無線感測網路[5]為其中一種技術。WSN 的發明是為了軍事的應用，可以偵測敵軍及生化武器的判定，如此可避免很多不必要的損傷。近年來，WSN 已經不侷限在軍事方面，WSN 被應用在許多領域，如：環境監測、健康照護等。無線感測網路中包含了大量的感測器,這些感測器具有感測、運算和無線通訊的能力，利用這些感測器收集資料，然後由基地台將這些資料彙整後，最後使用者能透過使用者介面得到資訊。雖然 WSN 的應用很大，不過它存在一個很大的缺點－資源有限(如記憶體、通訊頻寬和能量)。當 WSN 遭受 DoS/DDoS，攻擊者在短時間內傳送大量的封包到受害者，消耗其資源，使其無法正常運作。

前面提到，當 WSN 遭受到 DoS/DDoS 的攻擊，極易消耗頻寬和資源，造成網路癱瘓。如何解決此類的攻擊是一大挑戰，最簡單的方法，就是將攻擊者直接追蹤出來，且將此攻擊停止。但這類的攻擊往往會將原攻擊者的位址隱藏起來，利用別的位址，使受害者無法直接找出真正的攻擊者。在 IP 網路中，已經有許多方法是為了解決 DoS/DDoS 攻擊，其中有一個方法為 Edge Sampling [12]，此演算法利用機率標記封包，再由受攻擊的節點，從收集到的封包中的資訊，將攻擊路線找出。但 Edge Sampling 演算法需要收集到大量封包之後，方能重建攻擊路徑，這時 WSN 也許在找出攻擊者之前，已經消耗大量資源而導致網路癱瘓。基於此原因，本篇論文提出 H-PDF，利用機率的不同，達到減少收斂時間的目的(即重建攻擊路線所需封包的數目)，且利用此方法可以將同時發動的不同攻擊者找出。

本篇論文章節結構如下:第二節將提到在有關於 Traceback 的相關研究，第三節介紹如何將 Edge Sampling 套用到 WSN，第四節將透過 QualNet 比較 H-PDF 和 Edge Sampling 的效能，最後是結論。

2. 背景

在傳統的IP網路上有一種可以找出DoS/DDoS的原始攻擊者方法為IP Traceback，在這種方法中，又分為三類，分別為 Logging、ICMP-based 和 Probabilistic Packet Marking。不過由於WSN的資源有限，所以這些方法套用到 WSN 都有些缺點，如表 1。

Logging Traceback[1]會在一些路由器上將封包的資訊記錄下來，如：來源端的位址、終點端的位址等。當受害主機偵測到攻擊時，藉由比對攻擊者傳送的封包和紀錄的資訊找到攻擊路線。然而，這種方法需要大量的空間儲存資料。ICMP-based traceback[13]，這個方法是路由器會利用一個小的機率值決定是否產生額外的封包記錄此路由器的位址和他鄰近路由器的位址，然後傳送到終點端。終點端利用這些封包，將攻擊路徑找出。不過由於此種方法需要額外的封包存資料，會造成頻寬的負荷。Probabilistic Packet Marking，也是利用機率值決定是否標記封包，不過此法不會產生額外的封包。以 Edge Sampling 當例子，在 Edge Sampling 中，封包會被多加三個欄位 start、end 和 distance。當節點決定要標記經過的封包，他會將自己的位址寫入 start 欄位中，當封包經過下一個節點的時候，如果沒有被標記，此節點會將自己的位址寫入 end 欄位，再將 distance 欄位改為 1；假如節點決定要標記此封包，他就會將自己的位址寫到 start，而將前一個節點的位址覆蓋過。最後終點端利用這些資訊找出攻擊路徑。

在 Mobile Ad-Hoc Network (MANET)中，Jin 提出一個 Zone Sampling-Based Traceback (ZSBT) [18]，這種方法是將網路分割成幾個區域，每個區域有 ID，所以當節點決定要標記封包時，不是將自己的位址寫入，而是將自己所在的區域的 ID 寫入。因為在 MANET 上，節點是會移動的，如果只存區域 ID，更動的資訊可能會較少，不過所建構出的路徑較不正確。Thing 提出另一個方法為 ICMP Traceback with Cumulative Path (ICMP-CP) [14]，這個方法是基於 ICMP-based traceback，也是需要額外的封包傳送。在 WSN 中，Sy 和 Bao 提出 Coordinated Packet Trackback (CAPTRA) [4]，利用封包的廣播的特性，將封包記錄在多維度搜尋過濾器(Bloom Filter)，並利用「REQUEST-VERDICT-CONFESS」的訊息交換將攻擊路徑找出。不過這種方法不適合用於 DoS/DDoS 的追蹤。

由以上得知，追蹤 DoS/DDoS 的攻擊者並沒有最佳的方法，不過 Edge Sampling 為其中較佳的方法，我們的方法藉由改善 Edge Sampling 以減低收斂時間。

表 1 Traceback Algorithms for DoS/DDoS attacks

Approach	Algorithms	Deployment Environment	Weakness if applied in WSN
Hash-based	Logging (Hash-based) [1]	Conventional IP Network	• Require extra resources for downloading packet information from network routers • Require large processing and storage overhead
Hash-based Bloom Filter	CAPTRA[4]	WSN	• REQUEST-VERDICT-CONFESS message exchanges result in longer convergence time • Require specialized protocol to perform the message exchanges in each router • Not suitable for tracing the attacks with burst traffic
ICMP-based	ICMP-based traceback [13]	Conventional IP Network	• Expect a heavy IP protocol stack shall be onboard in each sensor
	ITrace-CP[14]	MANET	
Packet Marketing	Probabilistic Packet Marking [5]	Conventional IP Network	• Require a large amount of packets if the fixed probability is not selected properly
	Zone Sampling-Based Traceback [18]	MANET	• Less accurate attacking path reconstruction than conventional schemes

3. H-PDF 機制

WSN 的資源有限，所以要在 WSN 上發展防禦 DDoS 攻擊的方法，所消耗的資源必須比較少，在上節的 Traceback 各方法討論中，以種種跡象看來似乎 Edge Sampling 比較適用於 WSN，只要它能夠改進其收斂時間(即重建攻擊路線所需封包的數目)。基於此理由，本篇提出一套改進的 Hierarchical Probabilistic Dice Function (H-PDF)之機制。

WSN 由網路架構[7]可分為 Flat 網路和 Hierarchical 網路，在此篇論文乃著重於 Hierarchical 架構上。Hierarchical 和 Flat 的不同在於，在 Flat 架構上，每個感測器做的工作是一樣的，感測週遭環境之後將資訊傳到基地台；然而在 Hierarchical 的架構中，為了節省能量，將感測器分為兩層，網路被分為多個 cluster，在這種架構中，大部分的感測器的功用和在 Flat 架構上相同，但是在此時資料不直接傳到基地台，而傳給每個 cluster 裡面的 cluster head，cluster head 再將資料傳送到基地台。Cluster head 如何將資料傳送到基地台，有下列三種方法：

- 一般節點將封包傳給 cluster head，再由 cluster head 直接傳送到基地台，如 Low Energy Adaptive Clustering Hierarchy (LEACH) [16]。

- 一般節點將收集到的封包傳送到 cluster head，因為 cluster head 無法直接封包傳給基地台，故利用其他 cluster head 幫他將封包傳給基地台(如圖 1所示)。例如：Asymmetric communication and ROuting in Sensor networks (AROS)[8]。

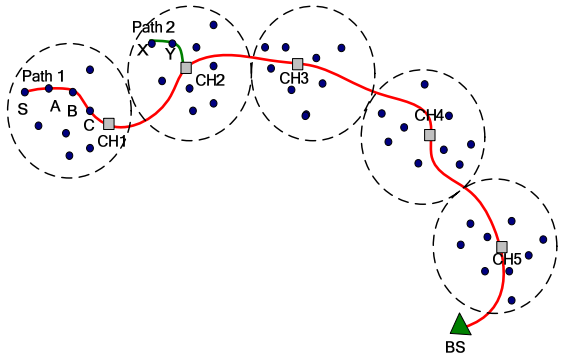

圖 1 Scenario of the attack path

- 一般節點同樣是將封包傳送給 cluster head，但 cluster head 互相通訊可能必須藉助在每個 cluster 間的邊界節點，利用這些邊界節點將封包傳送給另一個 cluster，最後傳到基地台。例如：Lowest-ID heuristic[2]

在本篇論文，我們以第二個方法做為模擬實驗模型，一般節點將封包傳送給 cluster head，之後透過 cluster head 間互相通訊，最後將封包傳至基地台，如圖 1。當攻擊者(Path 1)由 S 將封包傳出，S 位於 CH1 的 cluster 中，所以當封包傳到 CH1 後，就直接傳到下一個 cluster head CH2 然後再經由 CH3、CH4、CH5 最後傳到基地台。

在上節提到，Edge Sampling 是利用機率標記封包，當封包傳送到受害主機，再將這些標記過的封包收集起來，利用標記過的資訊將攻擊路線找出。通常 DDoS 攻擊會有許多攻擊者同時發動攻擊，假如每個攻擊路線皆未相交，Edge Sampling 是可以將攻擊者找出的，但是攻擊路徑可能會相交，所以 Edge Sampling 可能沒辦法發揮它的功能。因此，在 H-PDF 中，將封包的欄位的增加，除了在 Edge Sampling 中的三個欄位外，又多加了三個欄位 OriginCV、FirstCV 和 NextCV，以下為每個欄位所代表的意義：

- Start：封包被標記時節點的位址，可以被覆寫
- End：封包被標記後下一個節點的位址，也可以被覆寫
- Distance：封包標記的節點到距此節點最近的 cluster head 的距離
- OriginCV：封包所經過的第一個 cluster head 的位址，不可以被覆寫
- FirstCV：封包被標記後，經過的第一個 cluster head 的位址，可以被覆寫
- NextCV：FirstCV 的下一個 cluster head 的位址，可以被覆寫

H-PDF 演算法是改善 Edge Sampling 演算法之偵測能力，因為 cluster head 就像是圖學中的 cut-vertex，將 cut-vertex 拿掉，graph 會變成兩個 graph，所以 cut-vertex 就像是連接兩地 A、B 的橋一樣，要從 A 到 B 必須經過這座橋。因此 cluster head 就像橋一樣，封包一定會經過 cluster head。在這裡利用 OriginCV 這個欄位，可以很容易的將多個攻擊路線區別開來。如圖 1，有兩個攻擊路線，分別為 Path1 和 Path2，如果兩個攻擊同時發動，根據原本的 Edge Sampling 演算法是無法將兩條路徑辨別出，因為這兩條攻擊路徑有相交，如 CH2 做 packet marking 就會清除前面 sensor 所標記之資訊。但在 H-PDF 是可以將它分別開的，因為 Path1 的 OriginCV 欄位為 CH1，而 Path2 為 CH2，藉由 OriginCV，可以將這兩個攻擊路線辨別出來。FirstCV 和 NextCV 這兩個欄位可以較快速的找出的找出攻擊者所在的 cluster，然後封鎖此 cluster 傳出的封包。舉例來說，BS 接收到兩個攻擊封包，其包含(S,A,8,CH1,CH1,CH2)與(X,Y,5,CH2,CH2,CH3)的標記資訊，藉由 OriginCV 欄位便可判別攻擊路徑是來自於兩個不同的 cluster。

圖 2為一般節點如何標記封包，圖 3是當封包經過 cluster head 時如何運作，下面的例子是如何利用這六個欄位標記封包：在圖 1，Path1 的一個一般節點 A 決定要標記經過的封包，H-PDF 的欄位會變成(A,0,0,0,0,0)，當此封包經過下一個節點 B，如果 B 不標記，欄位為(A,B,1,0,0,0)，之後皆不標記，經過 CH1 時，欄位會變成(A,B,3,CH1,CH1,0)，經過 CH2 會變成(A,B,3,CH1,CH1,CH2)。如果在 B 時決定標記時，會將前面的標記覆蓋掉，欄位則會更改成(B.0,0,0,0,0)，

```
Marking procedure at normal node N:
  For each packet ω
  Let x be a random number from [0…1)
   if x< pi
     place 0 into all fields except for OriginCV
     write R into ω.start
   else
      if ω.distance = 0
           write R into ω.end
      if ω.FirstCV = 0
           increment ω.distance
```

圖 2 H-PDF Marking Procedure at Normal Node

```
Marking procedure at cluster head C:
  For each packet ω
    performs modified edge sampling
      if ω.OriginCV = 0
          write R into ω.OriginCV
          break
      if ω.FirstCV = 0
          write R into ω.FirstCV
          break
       if ω.NextCV = 0
          write R into ω.NextCV
          break
```

圖 3 H-PDF Marking Procedure at Cluster Head

在 Edge Sampling 中，每個節點被標記的機率是相同的，在 H-PDF 中，配置給一般節點和 cluster head 不同的機率，其 packet marking 機率如下：

- 一般節點：假設在 cluster 中有 i 個節點，一般節點的 packet marking 機率為

$$P_N = \frac{1}{\left\lceil \frac{i}{2} \right\rceil}$$

- cluster head：假設網路上有 C 個 cluster，則 cluster head 的 packet marking 機率為

$$P_c = \frac{1}{C+K}$$

其中 K 為正整數。

4. H-PDF 格式

在之前提到必須在封包中加六個欄位，但這六個欄位必須加在何處是接下來要討論的重點。IEEE1451[9]是規範感測器協定的標準，他定義了連接感測器標準到網路的介面，使得感測器有能力支援多種網路。在 IEEE1451 之下有 P1451.1、P1451.2、P1451.3、P1451.4、和 P1451.5 等子標準，其中 P1451.5 是定義無線傳輸的標準，因為要發展一套新的標準需要較久的時間，故 P1451.5 利用原有個無線傳輸的標準作為基礎，例如：IEEE 802.11、IEEE 802.15.1(Bluetooth) 和 IEEE802.15.4(Zigbee)，而[11]做了這三種標準的比較，其中 IEEE802.15.4[17]是為了實現 WSN 而提出的協定，他的電力壽命較長、花費較低且容易安裝。所以在此利用 IEEE 802.15.4 做為此方法的標準。

由圖 4，可看到 IEEE802.15.4 的封包格式分為五個欄位，分別為 Frame control、Sequence Number、Addressing fields (包含四個子欄位；Destination PAN ID、Destination address、 Source PAN ID、Source address)、data payload 和 FCS。由於除了 data payload 這個欄位外，其餘的欄位都無法更改，所以 H-PDF 利用 data payload 加入所需的欄位(如圖 5 所示)。PAN ID 可以用來辨別每個節點，在此標記的封包會將每個節點的 PAN ID 寫入需要填寫位址的欄位，所以只需要 2-bytes 記錄每個節點的位址，因此配給每個欄位 2-bytes 的空間，所以需要將 Data payload 這個欄位再切出 12bytes 的空間供 H-PDF 演算法使用。

2	1	4~20	variable	2
Frame control	SN	Addressing fields	Data payload	FCS

圖 4 MAC Frame Format in IEEE 802.15.4

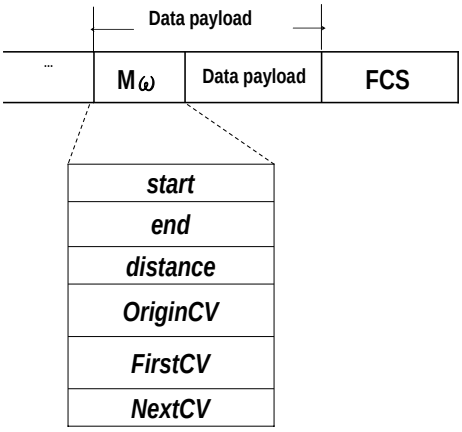

圖 5 Data Payload Field for H-PDF

上面提到如何放置演算法所需的欄位，此演算法還有一個問題未解決，即如何將不同的機率配置給每個節點。當 cluster head 選出時，cluster head 會有整個 cluster 的資訊，所以一般節點的機率由 cluster head 配置；而 cluster head 的機率則由基地台所配置。

利用 H-PDF，可以找出封包所經過的哪些 cluster，藉由封鎖發動攻擊的 cluster 也可以達到阻止 DoS/DDoS 的攻擊；如此雖然比較快速但卻可能造成網路的負擔，如果封包必須要依靠被封鎖的 cluster 的 cluster head 傳送，封鎖此 cluster，必須重新找路，所以在本篇論文，著重於將整條路徑都找出，如此找出的路徑是正確的且可以分辨出多條攻擊路徑。

5. 模擬

在此章節將利用實驗比較 Edge Sampling 和 H-PDF 的效能。利用網路中 cluster 的數目或每個 cluster 中節點的數目和收斂時間做比較。因為 DoS/DDoS 攻擊均在短時間進行完成，所以在實驗

中，我們假設網路拓樸不改變，也就是說，封包從某一點到基地台的路徑便不會改變，所以模擬利用同一條路徑，比較兩個演算法的收斂時間。在此利用 QualNet 做為網路的模擬工具，AODV 為路由協定。

首先，比較 cluster 的數目和收斂時間，先固定整個網路上節點的數目，在此設為 100，每個 cluster 中節點數目相同，在網路中 cluster 的數目分別為 1、2、3、4 和 5，比較 Edge Sampling 和 H-PDF，在此利用一般節點的機率和 Edge Sampling 的機率相等；以網路中 cluster 數目為 5 為例，每個 cluster 中的節點數目為 20，假設每個攻擊者經過一半的節點在此即為 10，然後再經由網路中的 cluster head 將封包傳送到基地台，則此路徑經過 14 個節點，一般節點的標記機率為 1/10，cluster head 的機率為 1/(5+k)，k 是常數在此設為 10。實驗結果如圖 6所示。

圖 6 Number of Cluster V.S. Number of Packet

由圖 6，得到下列兩點：

- 當 cluster 的數目越大，所需的封包數目越少
- H-PDF 的效能會比 Edge Sampling 好

第二個比較的是，Cluster Density (每個 cluster 中，節點的數目)和收斂時間。這次是固定 cluster 的數目，在此設定為 5，density 分別為 10、20、30、40 和 50，同樣的，每個 cluster 的節點數目還是相同；也是利用一般節點的機率和 Edge Sampling 演算法的機率相同。以 density 為 50 為例，一般節點的機率為 1/25，cluster head 的機率為 1/(5+k)，k 是常數在此亦設為 10，圖 7為得到的數值所繪出的比較圖。由圖 7，可以得到下列兩點：

- 當 density 越大，所需的封包數目越大
- H-PDF 的效能會比 Edge Sampling 好

由上面的實驗結果，可以得到 H-PDF 的效能會比 Edge Sampling 佳。

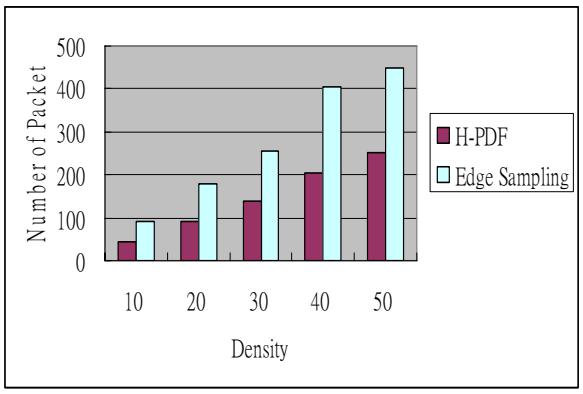

圖 7 Density V.S. Number of Packet

6. 結論

DoS/DDoS 此類的攻擊，會造成資源有限的 WSN 很大的損害，所以如何克服它對於 WSN 是很重要的課題。但是，在 WSN 上，如何追蹤攻擊者對於研究網路安全是一大挑戰。首先必須克服 WSN 的資源有限的問題，本篇論文利用在 IP 網路上原有的方法－Edge Sampling，因為這個方法較其他方法適合於 WSN。基於此理由，本篇提出一套改進的 Hierarchical Probabilistic Dice Function (H-PDF)之機制。H-PDF 可以利用其多加的三個欄位，可辨別出多個來自不同 cluster 的攻擊者。論文中運用 QualNet 網路模擬器對 H-PDF 做了驗證，實驗結果也顯示了 H-PDF 確實改善 Edge Sampling 之收斂時間。

參考文獻

[1] A.C. Snoeren, C. Partridge, L.A. Sanchez, C.E. Jones, “Hash-Based IP Traceback”, SIGCOMM’01, Aug 2001, pp.27-31.

[2] A. Ephremides, J.E. Wieselthier, D.J. Baker. “A design concept for reliable mobile radio networks with frequencyhoping signaling”. Proc. IEEE 75. 1987. pp. 56-73.

[3] C. Perkins, E. Belding-Royer and S. Das, “Ad hoc On-Demand Distance. Vector (AODV) Routing”, RFC 3561, July 2003.

[4] D. Sy and L. Bao, " CAPTRA: CoordinAted Packet TRAceback", The Fifth International. Conference on Information Processing in Sensor Networks (IPSN), Apr. 19-21, 2006.

[5] I. Akyildiz, W. Su, Y. Sankarasubramanian, and E. Cayirci, “A Survey on Sensor Network”, IEEE Communications Magazines, volume 40, pages 102–114, Aug. 2002.

[6] J. Kim, S. Radhakrishnan, S. K. Dhall: On Intrusion Source Identification. In: 2nd IASTED International Conference on Communications, Internet and Information Technology, November 17-19, 2003.

[7] Jamal N. Al-Karaki and Ahmed E. Kamal, “Routing techniques in wireless sensor networks: a survey”

[8] J. Neander, E. Hansen, M. Nolin, and M. Bj¨orkman, “Asymmetric multihop communication in large sensor

networks," in Proceedings of International Symposium on Wireless Pervasive Computing 2006 (ISWPC 2006), (Phukeet, Thailand), Jan. 2006.
[9] Kang Lee, "IEEE 1451 Standards for Smart Sensors", http://www.bfrl.nist.gov/WirelessSensor/index.htm#Smart_Sensors
[10] P. Ferguson and D. Senie. Network Ingress Filtering: Defeating Denial of Service Attacks Which Employ IP Source Address Spoofing. RFC 2827, May 2000
[11] Richard Hoptroff, "Zigbee for application developers"
[12] S. Savage, D. Wetherall, A. Karlin *et al*. "Practical network support for IP traceback", *In Proc.* of ACM SIGCOMM 2000, Santa Clara, 2000.
[13] Steven M. Bellovin, "ICMP Traceback Messages", Internet Draft: draft-bellovin-itrace-00.txt, submitted Mar. 2000, expiration date Sep. 2000,http://www.research.att.com/~smb/papers/draft-bellovin-itrace-00.txt
[14] V. L. L. Thing, H. C. J. Lee, M. Sloman, and J. Zhou, "Enhanced ICMP traceback with cumulative path," in Proceedings of 61st IEEE Vehicular Technology Conference (VTC '05), vol. 4, pp. 2415–2419, Stockholm, Sweden, May-June 2005.
[15] W. Feller. An Introduction to Probability Theory and Its Applications (2nd edition), volume 1. Wiley and Sons, 1966.
[16] Wendi Rabiner Heinzelman, Anantha Chandrakasan, and Hari Balakrishnan," Energy-Efficient Communication Protocol forWireless Microsensor Networks"
[17] Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs), IEEE std 802.15.4, Oct. 2003.
[18] X. Jin, Y. Zhang, Y. Pan, and Y. Zhou, "ZSBT: A Novel Algorithm for Tracing DOS Attackers in MANETS", EURASIP Journal on Wireless Communications and Networking, Vol. 2006, Article ID 96157, pp. 1-9, 2006.