加入有效點擊概念於 CCFDP 系統正確判斷有效點擊

林俐君
中國文化大學資訊管理學系
96707135@scenet.pccu.edu.tw

陳武倚
中國文化大學資訊管理學系
wuuyee@faculty.pccu.edu.tw

摘要

本文修正Collaborative Click Fraud Detection and Prevention (CCFDP) system的計分方式，除了原本無效點擊的證據外，加入有效點擊的證據，並對模型進行測試。測試內容包含模擬手動點擊與透過不同IP的機器人點擊(bot clicks)，以及CCFDP 系統在不同數目的時間分段下，手動點擊與機器人點擊點擊次數對分數的關係。結果顯示，點擊分數受到不同時間分段的影響，CCFDP在適當的時間分段下，能判斷出手動點擊與機器人點擊。

關鍵字：*Advertising；Click-Fraud；CCFDP*

1. 緒論

關鍵字廣告是計點擊次數付費（Pay per click／PPC），是一種廣告模型廣泛用在搜尋引擎、廣告網路、以及網站或部落格。當網際網路使用者點擊廣告主刊登的廣告時，廣告主才需付費。廣告主向關鍵字廣告代理商競標他們認定目標市場對象在尋找某個產品或者服務時，也就是網際網路使用者，可能會於搜尋列鍵入的關鍵字。當使用者鍵入關鍵字查詢與廣告主的列表匹配、或者檢視某相關內容的網頁，該廣告主投放的廣告就會顯示。它通常出現於搜尋結果網頁或者隨機出現在結果頁的任何地方，網管或部落格主決定廣告放於內容頁的位置。點擊付費廣告也有可能在聯播網站內容中出現。在這種情況下，廣告網路像Google Adsense與Yahoo! Publisher Network會嘗試提供與該頁該廣告應出現位置及週遭內容相關的廣告。所以不需要透過搜尋功能也能有廣告效果。

Google AdWords、雅虎搜尋行銷、與微軟adCenter三大網路業者，根據搜尋引擎不同，最低價以美金1分到50分起標。在搜尋引擎裡流行熱門的詞價位相對較高。計次點擊付費廣告目前最具爭議的是利用關鍵字廣告開啟了惡意點擊的議題。

根據專門偵測廣告點閱詐欺（click fraud）的Click Forensics公佈2010年第四季度的總體點擊欺詐率下降到19.1%，但2010年第三季為22.3%，高於2009年第四季15.3%、2008年第四季17.1%，2007年第三季的16%，以及2006年第四季的16.6%。Google及Yahoo曾因點閱詐欺而被廣告主告上法庭，所以如何區分出惡意點擊（click fraud）是在這龐大營收下，不得不重視的議題。

Google及Yahoo搜尋引擎會面臨「惡意點擊」的指控原因，主要是來自於：

1. 廣告主的商業競爭對手，藉由製造大量的詐欺點閱量，用完廣告主的廣告預算，讓廣告下架打擊對手。

2. Google、Yahoo等搜尋引擎業者所合作的加盟經銷商，藉著增加點閱量，增加廣告主的廣告費用支出，藉此拆得更多佣金。

這兩項主要被指控的原因，對於搜尋引擎而言也很無奈，但是既然提供服務就必須做好預防措施這也是搜尋引擎的責任，所以目前提供關鍵字付費廣告PPC的搜尋引擎也都已經提供廣告主點擊詐欺的過濾程式，但是這無法治本只能治標。

面對關鍵字廣告業者的競爭對手惡意攻擊，搜尋引擎所提供的過濾程式並不是主動的幫刊登廣告者將疑似有問題的點閱費用移除，而是讓關鍵字廣告代理商及廣告刊登者自行提出疑問，如果真有問題再扣除費用。

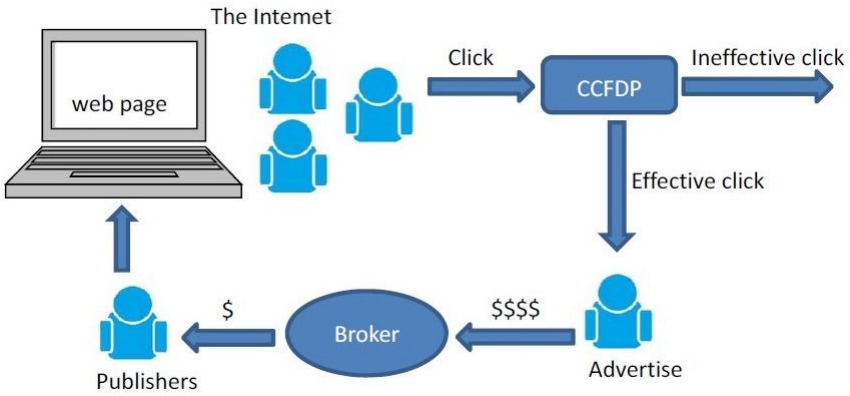

圖1. 關鍵字廣告的商業模式：由廣告客戶向廣告仲介付費，仲介轉向刊登業主並刊登於網頁，大眾透過網路點擊網頁，將點擊數據經CCFDP系統區分為有效與無效點擊，廣告客戶依照有效點擊的次數付費給仲介。

CCFDP系統(Kantardzic, Walgampaya et al. 2010)，是以統計為基礎做預測及分析，必須要累積一段很長的時間，以獲取統計上的意義。然而一般的部落格廣告或關鍵字廣告並非長時間刊登同一個廣告，就某間關鍵字廣告公司累積的客戶資料去分析，刊登時間通常不超過三個月，在廣告時間不長，數據累積不足的情形下，CCFDP系統是否仍適用，成為一重要課題。

本文我們就某間關鍵字廣告公司累積的客戶資料去分析，並且定義並探討何謂手動惡意點擊與機器人惡意點擊，依此點擊模式，以人為方式將點擊數據加入click data，來測試CCFDP系統是否可以正確判斷出惡意點擊的程度。其中我們修改計分方式，加入有效點擊的證據的概念。最後我們將進一步探討時間分段的問題，找出適合的分段方式。

2. 相關研究

近幾年來如何防範惡意點擊的研究相當熱門，國際期刊例如Kantardzic 利用數據融合增進惡意點擊的判定(Kantardzic, Walgampaya et al. 2008)，例如Hamed Haddadi 使用Bluff Ads防止線上的惡意點擊(Haddadi 2010)，Immorlica et al. 透過分析點擊欺詐學習算法，計算估計點擊率。(Immorlica, Jain et al. 2005)。在2010年，Mehmed Kantardzic 等人提出CCFDP系統，藉由數據融合增加點擊判定的正確性(Kantardzic, Walgampaya et al. 2010)。Juels et al.藉由優質點擊(premium clicks)來防止惡意點擊 (Juels, Stamm et al.

2007)。國內亦有不少論文探討相關研究。透過偵測與清除程式防禦殭屍病毒讓使用者能夠安心操作電腦(黃博緯 2012)、分析受害電腦在網路活動中找出網路行為特徵偵測機器人點擊(張宗銓 2012)、以TCP Splicing技術為基礎來進行點擊詐欺的防禦、利用點擊門檻分析演算法進行點擊詐欺的偵測(張源平 2006, 闕維論 2010)、導入的新型金鑰管理在P2P Botnet(蘇文輝 2009)。

3. 何謂無效點擊與有效點擊

此處的界定並非以點擊者的心理狀態決定，因為我們並無法了解點擊者在點擊的那一刻的想法是否為惡意，因此不可能明確界定哪些點擊為無效的惡意，哪些點擊為正常有效的點擊。

為達到公平的計分方式，此處以常態做為基準。舉例而言，長時間統計下，平均一天有100個點擊，且變異數為20個點擊，如果某點即次數爆增為200次，此時我們就視為非常態，就算點擊者非惡意，我們也將此視為無效點擊的證據，點擊數目越多，無效點擊的證據越大，反之，若點擊次數為50次，我們則視為有效點擊的證據。

4. 何謂無效點擊與有效點擊

4.1 評分原則

文獻提供的評分方式(Kantardzic, Walgampaya et al. 2008)依據超過正常點擊，視為有證據顯示為無效點擊，並且以0分表示沒有證據顯示為無效點擊，1分為100%有證據為無效點擊。

然而這樣的評分方式並不公平，超過常態的點擊次數的點擊視為無效點擊的證據，低於常態點擊次數的點擊也應該視為有效點擊的證據。因此，此處我們以0.5分視為沒有任何證據顯示為有效或無效點擊，以高於0.5分視為無效點擊的證據，低於0.5分視為有效點擊的證據。.在此計分方法下，1分為有100%證據為無效點擊，0分表示有100%證據為有效點擊。

4.2 評分原則

N：總點擊數

p_i：第i時間分段佔總時間的分數

s_j：屬性分段下的點擊數

c_i：時間分段下的點擊數

$x_{i,j}$：時間及屬性分段下的點擊數

σ_j：時間及屬性分段下變異數

$U_{i,j}^{\pm}$：時間及屬性分段下無任何證據的上限與下限

$$\sigma_j = \sum_{i=1}^{n} p_i \left(\frac{x_{i,j}}{c_i} - \frac{s_j}{N} \right)^2 \quad (1)$$

$$U_{i,j}^{\pm} = \left(s_j / N \pm 1.645 \times \sigma_j \right) \times c_i \quad (2)$$

$$score_{i,j} = \begin{cases} \frac{x_{i,j} - U_{i,j}^{+}}{2c_i} + 0.5 & \text{if} \quad x_{i,j} \geq U^{+}{}_{i,j} \\ 0.5 & \text{if} \quad U^{-}{}_{i,j} \leq x_{i,j} \leq U^{+}{}_{i,j} \\ \frac{U_{i,j}^{-} - x_{i,j}}{2c_i} + 0.5 & \text{if} \quad x_{i,j} \leq U^{-}{}_{i,j} \end{cases} \quad (3)$$

舉例說明，總點擊數 N 為339次，將時間分成兩個區段，c_1 時段內的點擊數為192次，c_2 為147次。將IP分成三個區段，s_1 區段內的點擊數為143次，s_2 為82次，s_3 為114次。若同時以時間與IP區段來劃分，則可以得到六個 $x_{i,j}$ 區段的點擊數。

表 1. 將總點擊數依時間與 IP 區段區分為 6 個部份。

	總點擊次數	第一段 IP 區間	第二段 IP 區間	第三段 IP 區間
總天數	$N=339$點擊次	$s_1=143$點擊次	$s_2=82$點擊次	$s_3=114$點擊次
第一天	$c_1=192$點擊次	$x_{11}=98$點擊次	$x_{12}=50$點擊次	$x_{13}=44$點擊次
第二天	$c_2=147$點擊次	$x_{21}=45$點擊次	$x_{22}=32$點擊次	$x_{23}=70$點擊次

每個時間分段佔總時間的分數為： $p_1 = p_2 = \frac{1}{2}$

表 2. 不同 IP 分段下的標準差

	第一段 IP 區間	第二段 IP 區間	第三段 IP 區間
標準差	$\sigma_1=0.010618$	$\sigma_2=0.000464$	$\sigma_3=0.015524$

表 3. 不同時間及 IP 分段下的計分方式的上限及下限

	第一段 IP 區間	第二段 IP 區間	第三段 IP 區間
第一天	$U_{1,1}^{+}=84.34$	$U_{1,2}^{+}=46.59$	$U_{1,3}^{+}=69.47$
	$U_{2,1}^{+}=64.58$	$U_{2,2}^{+}=35.67$	$U_{2,3}^{+}=53.19$

	第一段 IP 區間	第二段 IP 區間	第三段 IP 區間
第二天	$U_{1,1}^{-}=77.64$	$U_{1,2}^{-}=46.30$	$U_{1,3}^{-}=59.66$
	$U_{2,1}^{-}=59.44$	$U_{2,2}^{-}=35.45$	$U_{2,3}^{-}=45.68$

表 4. 不同時間及IP分段下的分數

	第一段 IP 區間	第二段 IP 區間	第三段 IP 區間
第一天	$score_{1,1}=0.54$	$score_{1,2}=0.51$	$score_{1,3}=0.46$
第二天	$score_{2,1}=0.45$	$score_{2,1}=0.49$	$score_{2,3}=0.56$

由上述的分數顯示，某些區段內小於0.5，有證據為無效點擊，某些區段內大於0.5有證據為有效點擊。

5. 數據融合

點擊數據的屬性可以是IP、廣告主與作業系統等，數據融合的目的是將這些不同屬性做融合，以得到更正確的分數。此處使用Dempster-Shafer(Dempster 1967, Shafer 1976)理論來融合數據。由於點擊區分為有效點擊與無效點擊，Frame of discernment只有true與 fraud 兩種，因此Dempster-Shafer的計算可化簡為下式：

$$S=\frac{\prod_{=1,n} r_i}{\prod_{=1,n} r_i+\prod_{=1,n}(1-r_i)} \tag{4}$$

舉例而言，某個點擊的IP分數為0.5分，廣告主分數為0.7分，數據融合後的分數計算如下：

$$S=\frac{0.5\times 0.7}{0.5\times 0.7+(1-0.5)\times(1-0.7)}=0.7$$

在數據融合時，當某個屬性不論其分數大小，與另一個0.5分的屬性融合後，最終分數將維持不變。此結果與定義相符，當沒有任何證據顯示為有效或無效點擊時，此一屬性融合後不影響最終結果。

再舉一例說明，若某個點擊的IP分數為0.4分，廣告主分數為0.7分，則數據融合後分數為0.61分，此為有效點擊與無效點擊互相影響的結果，融合後的分數將介於兩者之間。

6. 時間分段的方法

時間分段的方式分成兩種，第一種方法是以點擊總時間為主，將總時間平均分成多段，再統計各段時間內的總點擊數。計算後每段時間內的點擊數不同，時間長度相同。第二種方法為以總點擊數為主，將總點擊數平均分成多段，再計算每個點擊區段的時間，計算後每段時間內的點擊數相同，時間長度不同。

分數由兩個重要變數決定：

1.變異數σ_j的大小。

2.每個時間及屬性分段下的點擊數$x_{i,j}$的差異。

將時間段數分越多段，怎每一段的差異越大，σ_j越大。例如有些時段有數百個點擊，有些時段可能只有數十個點擊。同樣點擊數$x_{i,j}$的差異也因時間段數分越多段而越大。

以總點擊數為主的分段方式，可確保每個時間分段中的點擊數相同，因此σ_j的大小主要為點擊數$x_{i,j}$的差異。

7. 實驗結果

數據來源為某個部落格廣告公司所提供。此廣告刊登為期兩個月，總點擊次數約一萬次。click data中每個點擊的欄位包括廣告主、IP位置及點擊時間。依循上述的計分方法後得出每個點擊的分數。

7.1 原始數據的分數統計

結果顯示，依總時間平均分段的點擊中，由於$x_{i,j}$的差異增加，因此分成 30 段比分成 10 段的分數的分布範圍更廣。然而分成 50 段時，因為σ_j增加的幅度高於$x_{i,j}$的差異，而σ_j增大會拉大無任何證據的上限與下限的差距，因此分數大都集中在 0.5 分。

以總點擊數為主的分段方式則是因為σ_j的大小主要為點擊數$x_{i,j}$的差異，因此分段數越多，分數分佈範圍越廣。

由以上結果得知，分數的大小將受分段方式不同而不同。但是整體的分布仍接近常態分佈，左右對稱。

如果將超過0.6分作為判定是否為惡意點擊的標準顯失公平，因為同樣低於0.4分的點擊也相當多。超過0.6分有可能是因為分段數不同造成分數分布變廣，而非是惡意點擊。

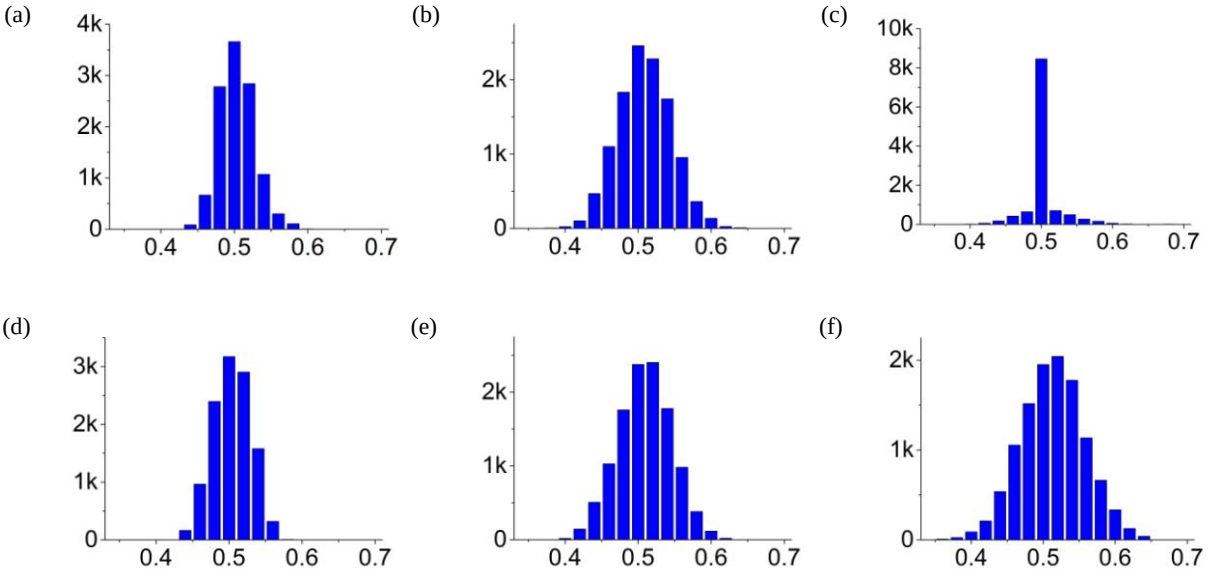

圖2. 縱軸為總點擊數，橫軸為分數，(a),(b),(c)的計分過程中，依總時間平均分段，分別將時間分為10段、30段、50段。(d),(e),(f)則是依總點擊數平均分段，同樣分別將時間分為10段、30段、50段。

7.2 模擬同一時段內手動點擊的結果

段數多的時候(50段)，鑑別效果比總時間平均的分段的結果好。

圖(g)與(h)分別為以總時間平均的分段與以點擊數為主的分段在加入不同點擊次數時，這些額外加入的點擊的分數。在點擊次數為10次時，分數約在0.6分，接近常態分佈的最大值，亦即點擊在10次以內，我們都無法分辨是否屬於常態分佈。

隨著點擊次數增加，分數也隨之增加，增加的速度依分段方式與分段數而不同。分段數越多，分數增加越快，效果越好。

整體而言以點擊數為主的分段方法分成50段的結果最適合分辨出手動點擊的部分。

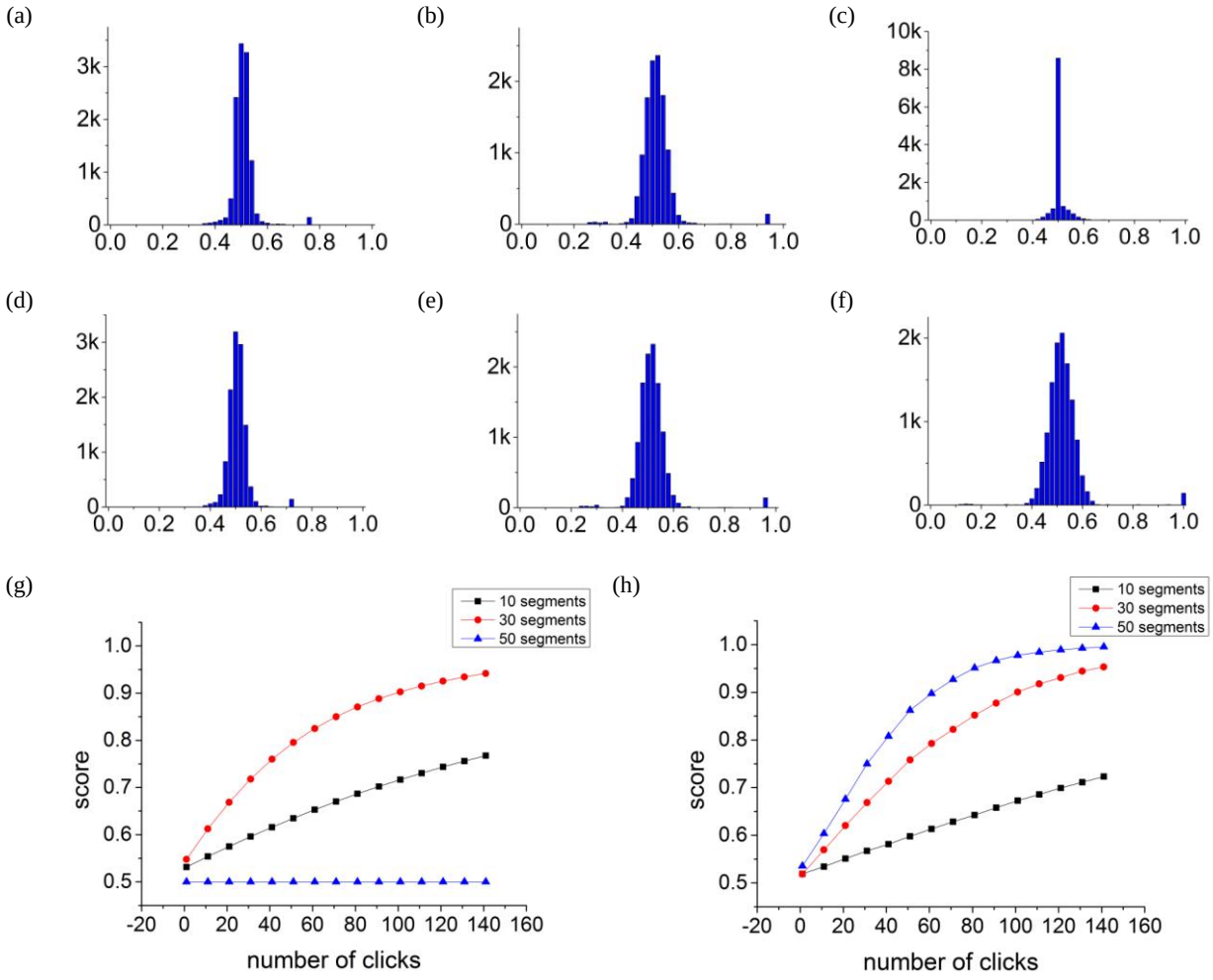

圖3. 同一個IP address在同一個時段內，在click data中加入點擊140次的點擊數據，並統計所有點擊的分數分布。所加進去的點擊總數約占原始數據的1%左右。圖二各圖的分段方式與時間分段數與圖一相同。

7.3 模擬分布於同一時段內機器人點擊(bot click)的結果

結果顯示，因為透過不同IP點擊，因此這些點擊的分數不盡相同，分布也是接近常態分佈，但是平均值高於0.5分，因此可以輕易辨別出來是否為有效點擊。

與圖二相比，不論是以總時間平均的分段或是總點擊數為主的分段，如果只透過1個 IP在同一時段內點擊10次，則分數落在0.6分以下，圖三則顯示，如果同一時段內，雖然每個IP都一樣只點擊10次，但是120個IP的點擊造成這個時段內的總點擊數異於常態，所以仍然可以由分數的分布，清楚將這些點擊辨別出來。

圖三的(g)(h) 是將1200個點擊次數，平均分配到不同IP addresses，再將每個IP的平均分數計算出來，例如第一個點是同一個IP 點擊1200次，第二個點是10個 IP addresses點擊120次，以此類推。(g)(h)的差別在於(g)是以總時間平均的分段，而(h) 是以總點擊數為主的分段。

結果顯示以總時間平均的分段方式，平均分數與分段的次數有關，分段越多平均分數越高，但是分段太多則造成變異數過大，因此分數集中在0.5分。以總點擊數為主的分段方式一樣是分段次數越多，平均分數越高，但是差異不大，並且分數都在0.8分以上。

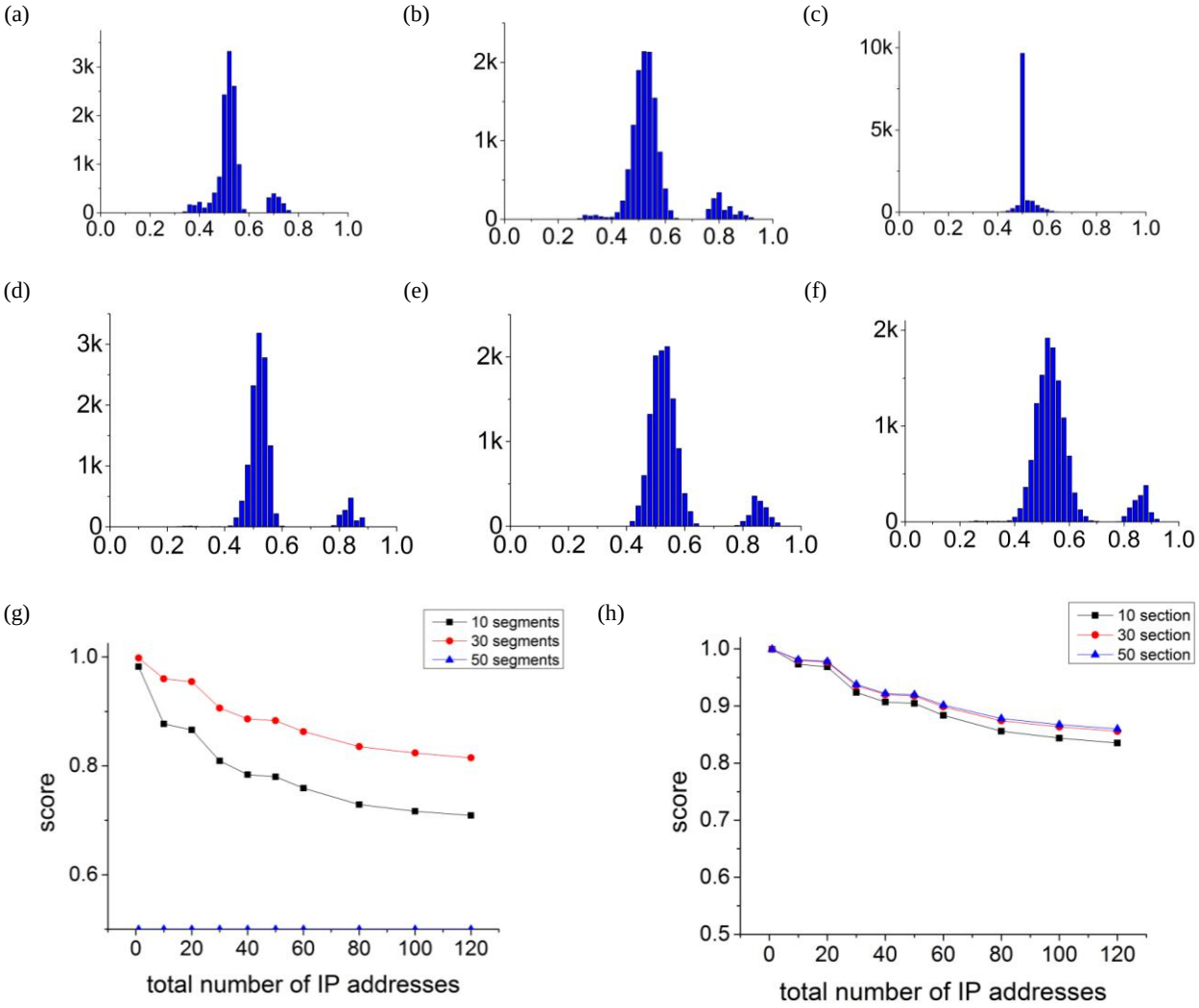

圖4. 120個IP address在同一個時段內，在click data中分別加入點擊10次的點擊數據，並統計所有點擊的分數分布。所加進去的點擊總數為1200筆，約占原始數據的10%左右。圖三各圖的分段方式與時間分段數與圖一相同。

7.4 模擬分布於不同時段內機器人點擊(bot click)的結果

結果顯示，不論是以總時間平均的分段或是總點擊數為主的分段，若點擊時間分布於總時間的1/10時，勉強可以鑑別出無效點擊的部分，平均分數在0.7分左右，分布於總時間的1/5時則不明顯，分布於總時間的1/4時則完全無法辨識。這代表CCFDP系統將會

把這樣的點擊模式視為常態點擊。

圖四的(g)(h) 是將1200個點擊次數，平均分配到不同IP addresses，再平均分配到不同的時段範圍內，最後將所有IP的平均分數計算出來，例如第一個點是同一個IP 點擊1200次，第二個點是10個 IP addresses點擊120次，以此類推。

(g)(h)最左邊的起始點代表只有1個IP，分布在不同時間長度內的點擊。結果顯示，雖然只有一個IP，但仍受時間分布長度的影響，但點擊平均分數皆在0.8分以上，所以仍可分辨出是否為有效點擊。

整體而言，不論是分成幾個IP addresses 的點擊，分布時間越廣，額外加入的點擊的平均分數越低。如果bot click分布在超過1/4的範圍，並且超過30個IP作為點擊，則點擊平均分數在0.8分以下。

此結果並不令人感到意外，因為CCFDP系統將持續穩定於整個統計時段的點擊數視為常態，因此如果惡意點擊的型態為透過不同IP，並且刻意每次都點擊相同數量，持續執行一段很長的時間，系統將無法分辨出為常態點擊或惡意點擊。

然而這樣的惡意點擊也不容易成功，因為一但開始點擊就必須一直持續下去，中途不能停止也不能增加，而且必須執行超過整個廣告刊登時間的1/5，一般不容易達到上述條件，因此CCFDP系統除了上述的特例外，可以辨別出大部分的bot click。

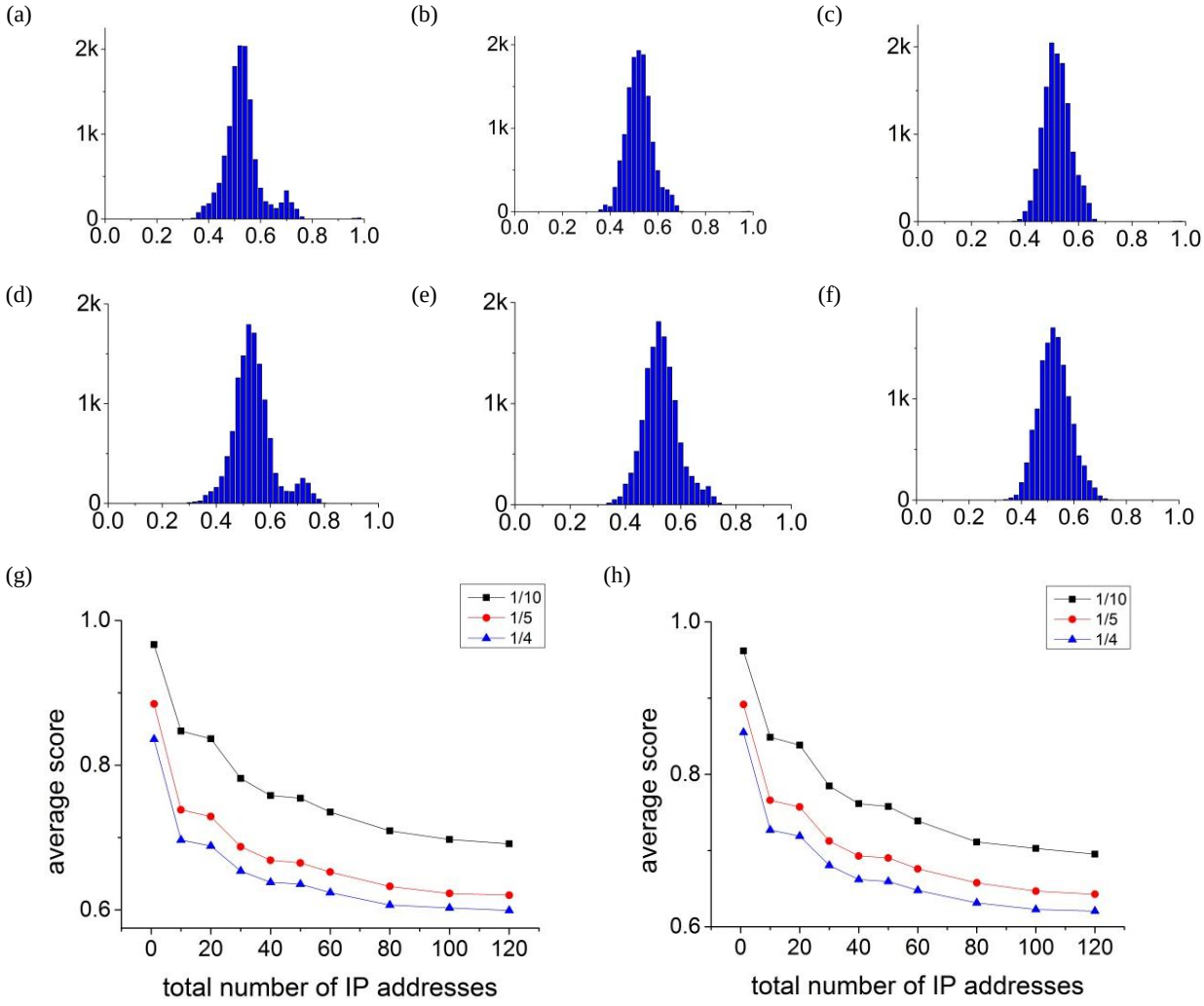

圖5. 120個IP address在不同時段內，在click data中分別加入點擊10次的點擊數據，點擊時間平均分布於總時間的1/10、1/5及1/4範圍內，最後統計所有點擊的分數分布。所加進去的點擊總數為1200筆，約占原始數據的10%左右。

8. 討論與未來展望

由於不同的時間分段下，產生的數據結構完全不同，CCFDP系統的計分結果深受分段方法的影響。

由上數的計分結果我們可以發現，引入有效點擊的證據，可以藉由整個分數統計而得到一個分布結果，藉由比較分數超過0.5分與分數低於0.5分的分布，我們可以判斷是否為因為分段數的不同，而造成點擊分數變化，因此可以據此判斷是否為異於常態的點擊。

以總時間平均的分段，每段時間的長度都一致，然而時間分段並不需要同等長度，只要依不同長度做等比例調整權重即可。舉例說明，長時間刊登某個廣告，一開始時可能點閱率不高，而後期時點閱數字大幅提升，此時如果仍將時間等長度切割，可能會造成變異數增加。此為以總時間平均分段的缺點，結果顯示以總點擊數平均的分段則可避免此問題。

以總點擊數作為分段方式不論在分離同一時段內的手動點擊或bot click，效果都優於以總時間作為分段的方式。以總時間作為分段的方式還需要注意是否分段數過多，造成分數集中於0.5分。以總點擊數作為分段方式的分段數過多的話，將造成整個點擊分數的分佈更廣，但仍可有效分辨出惡意點擊。

由上述結果顯示，透過click data可以有效分離出惡意點擊的部分，並且也點明，若以長時間分布，多個IP點擊，則只使用上述的click data，仍有不足之處。

將來可再增加其它點擊屬性，例如所使用的瀏覽器、作業系統等，可以使CCFDP系統更加完善。

9. 結論

在這篇文獻中，我們改良了CCFDP系統的計分方式，並透過模擬測試是否可以分離出無效點擊。

藉由改變時間的段數，我們可以將CCFDP系統應用在短期廣告，在統計次數有限的情形下，得到最佳且合理的計分，使CCFDP系統使用範圍不再限於長時間的廣告。

測試結果除了惡意點擊方式以長時間分布且數目固定的方式點擊外，皆能有效分離出無效點擊。

參考文獻

Dempster, A. P. (1967). "Upper and lower probabilities induced by a multivalued mapping." The annals of mathematical statistics **38**(2): 325-339.

Haddadi, H. (2010). "Fighting online click-fraud using bluff ads." ACM SIGCOMM Computer Communication Review **40**(2): 21-25.

Immorlica, N., et al. (2005). "Click fraud resistant methods for learning click-through rates." Internet and Network Economics: 34-45.

Juels, A., et al. (2007). Combating click fraud via premium clicks. Proceedings of 16th USENIX Security Symposium on USENIX Security Symposium, USENIX Association.

Kantardzic, M., et al. (2008). Improving click fraud detection by real time data fusion. Signal Processing and Information Technology, 2008. ISSPIT 2008. IEEE International Symposium on, IEEE.

Kantardzic, M., et al. (2010). Click Fraud Prevention via multimodal evidence fusion by Dempster-Shafer theory. Multisensor Fusion and Integration for Intelligent Systems (MFI), 2010 IEEE Conference on, IEEE.

Shafer, G. (1976). A mathematical theory of evidence, Princeton university press Princeton.

張宗銓 (2012). 在網路行為中以 PSO+K-means 偵測殭屍網路之機制. 事業經營學系(所). 台北市, 大同大學. **碩士:** 69.

張源平 (2006). 建構於系統核心之點擊造假攻擊防禦系統. 資訊工程研究所, 國立中央大學. **碩士:** 39.

黃博緯 (2012). Koobface 殭屍網路防禦機制之研究. 電機工程系. 台北市, 國立臺灣科技大學. **碩士:** 74.

闕維論 (2010). 線上關鍵字廣告之點擊詐欺研究. 資訊管理學系. 台北市, 中國文化大學. **碩士:** 61.

蘇文輝 (2009). 基於新的金鑰管理建構P2P Botnet. 資訊管理系碩士班. 雲林縣, 雲林科技大學. **碩士:** 55.