模糊最短路徑應用於犯罪網路模型之研究

The study of using fuzzy shortest path on criminal network model

張明桑
中央警察大學資訊管理學系副教授
大崗村樹人路 56 號
桃園縣 33304 龜山鄉
mschang@mail.cpu.edu.tw

郭俊億
中央警察大學資訊管理學系研究生
大崗村樹人路 56 號
桃園縣 33304 龜山鄉
im973084@mail.cpu.edu.tw

林中昱
中央警察大學資訊管理學系研究生
大崗村樹人路 56 號
桃園縣 33304 龜山鄉
im963094@mail.cpu.edu.tw

摘要

隨著時代的演變，犯罪的型態不斷的推陳出新，從個別性犯罪到組織性犯罪的改變，組織性犯罪活動的威脅與其所造成的嚴重經濟混亂，至今仍沒有一個國家可以自外於這個日趨嚴重的問題。而如果我們再以傳統偵查方式來偵辦的話，將更耗時與費力。因此本文提出一個應用社會網路分析和模糊數學的方法來偵查組織型犯罪，其優點爲偵查的成本不因人犯潛逃或證據被湮滅而損失過多，另外並利用模糊數學的特性來使偵查更具彈性、更符合實際需要。而本篇所解決的問題有下列二個：

第一：利用兩種模糊最短路徑方法來尋找最佳偵查路徑：根據不同的情形使用不同的方法，以符合實際需要和達到節省偵查成本的目的。

第二：尋找這條最佳偵查路徑的最關鍵邊(most vital edge)：在偵查過程中常常發生人犯潛逃或證據被湮滅的例子，這個方法可以使偵查人員先針對最關鍵邊做偵查，以爭取犯罪證據的時效性。

目前在犯罪偵查上，所能利用的軟體並不多，有些軟體以圖像式的方式來做關聯，並不具有分析的功能，本文即希望可以分析這些組織犯罪，並以最少成本來達到犯罪偵查的目的。

關鍵詞: 組織性犯罪、模糊數學、最短路徑、最關鍵邊(most vital edge)

Abstract

Criminal types have changed from individual crimes to organized crimes. The organized crimes threaten and cause serious economic disruption. No country can avoid this growing problem. It will cost much time and labors if we still use traditional approaches to investigate organized crimes. Therefore, we propose methods of using an application of social network analysis with fuzzy method to detect organized crimes. The advantage of our methods is that it won't increase too much investigative cost due to the criminals escape overseas or be murdered etc. In addition, the usage of the characteristics of fuzzy mathematics makes detection more flexible and practical. This paper wants to solve the following two problems:

First, we use two types of fuzzy shortest path to find the best path to investigate crimes. It is based on using different ways to handle different situations. It achieves the goal to meet the actual needs and cost savings in the investigation.

Second, we will find the most vital edge in the best path. In the investigation process, the criminals often escape or evidence is destroyed. This method will enable investigators to detect the most vital edge and achieve the efficiency of the security of criminal evidence.

At the present time, there is not much software created for the usage of the investigation of crimes. Some software tools can only visualize criminal network and do not offer much help with association search. This paper will analyze the organized crimes and achieve the goal of cost savings in crime investigation.

Keywords: Organizational crime, Fuzzy mathematics, the shortest path, most vital edge

壹、緒論

時代的演變，犯罪的型態日新月異，從簡單改變到複雜組織性犯罪型態，造成的嚴重經濟混亂，世界各國均無倖免。然而組織犯罪案件與日俱增且犯罪模式、手法日益複雜，愈來愈多的刑案，偵查人員無法從犯罪現場獲得關於案情的相關跡證，自然無法經由有效的線索來偵破刑案。

自從美國 911 事件以來，各國安全部門及單位就十分重視組織犯罪資料的搜集、挖掘和相關數據資料庫的建立，以歷史資料爲基礎，並利用資訊擷取與連結分析技術，找出犯罪的特徵，提供隱藏的線索，協助破案及遏止犯罪，因此相關執法部門及情報搜集部門意識到掌握組織性犯罪之網路結構，對於犯罪偵查是相當重要的。

爲了瓦解組織犯罪，我們必須找出誰是犯罪的主導者，爲了此目的，必須先了解整個犯罪網路架構中成員間的關聯，才能真正有效的打擊犯罪組織；另一方面，國內外基於社會網路分析來針對犯罪組織的研究少之又少，因此本篇論文將以社會網路分析爲基礎，並結合模糊理論來研究犯罪組織的內在網路關係，我們稱之爲犯罪網路模型(criminal network model,簡稱 CNM)之研究，希望能在此一範疇開創新視野，並達到拋

磚引玉的效果。

我們可以把犯罪者視爲一個網路，犯罪世界如同是社會生活系統的一部份，犯罪組織成員之間所建構的網路關係亦是社會複雜網路結構中的部分組成，在網路中他們互相影響，並且扮演不同的腳色，而在這些個體之間的關聯是揭露犯罪活動和打擊犯罪的重要部份，爲了瓦解犯罪組織，偵查人員可能要花費大量的時間來從資料庫中作搜尋，閱讀犯罪報告及尋找犯罪者之間相關聯的線索。爲此，犯罪調查人員通常利用一種方法，這方法稱爲連結分析法(link analysis)，它能協助偵查的引導和揭露疏漏的資訊。

雖然市面上有一些套裝軟體標榜著具有連結分析功能，但是他們僅是提供犯罪網路的視覺表示方式，並沒有實際上從事分析的能力。因此本研究最主要的問題，在如何於犯罪網路圖形中，以社會網路分析爲基礎，並結合 fuzzy 理論，提出適合的演算法來尋找犯罪網路模型中最佳的偵查路徑及其替代機制。

貳、文獻探討

一、組織犯罪偵查

犯罪偵查向來被視爲較爲冷僻之研究領域，乃因爲其本質上具有相當濃厚之實務成分，一般研究亦多將重點置於各類偵查技術之法律基礎，鮮有真正對於實務偵查活動內容進行剖析。以組織犯罪偵查而言，因組織犯罪防治條例係屬創新立法，並融合諸多國外先進之抗制組織犯罪經驗與做法，於國內司法運作實務上，包括警察、檢察機關，乃至於法院均尚處於摸索階段，有賴以偵查實務爲基礎，藉由案例之累積，逐漸形成解釋與判例達成共識。

另外，相關研究與偵查實務均指出，對抗組織犯罪之困難程度遠超過任何單一之謀殺案，其可能包括長時間連續對於毒品交易、色情娼妓處所之搜捕，以及揭發隱藏其中之犯罪企業集團，偵查人員必須能偵測並發現組織犯罪的存在，熟捻組織犯罪之法律構成要件，進而藉由偵查蒐證已發展顯著的證據。以美國抗制組織犯罪經驗爲例，早期執法機關很少以連續性之作爲對於組織犯罪團體加以偵查起訴，當輿論與公眾的壓力大時，執法機關就以偵查起訴，當公眾注意力降低時，執法就相對鬆懈，此點與國內情形頗爲相似，其主要的原因在於大多數司法警察機關對組織犯罪偵查仍顯生澀，且關於組織犯罪偵查蒐證方式、犯罪事實之採證與認定等偵查實務，亦未充分瞭解司法審檢機關之認知與態度。反之，司法機關對於組織犯罪之生態運作以及偵查實務，亦多未能真正深刻體認，造成警察、檢察、法院三者之間的落差，恐有礙於組織犯罪之偵查，進而影響組織犯罪條例抗制組織犯罪之功能。基於上述理由，爲協助警察機關，以正當、有效、合法之偵查活動抗制組織犯罪，期能建構一套足以有效抗制組織犯罪的偵查模式。

二、社會網路

(一)社會網路分析(social network analysis, 簡稱 SNA)

根據 Scott[7]的溯源性分析指出，社會網路的發展起源自三個主要學術傳統的累積：首先爲德國計量社會分析學家著重於小團體研究，並進而創造許多科技先進的計量技巧配合圖形理論(graph theory)所產生的研究取向。第二，根源於 1930 年代的哈佛研究者探索個人關係的模式與次級團體的形成。第三，形成於曼徹斯特社會人類學的研究

學者，基於上述的論點用於考察土著及小村落社會的社區關係結構模式。而這些多元理論性分析的發展路徑最後於 1960 到 1970 年代之間在哈佛大學再次產生學術的匯集，進而逐漸建構與形塑出當代社會網路的分析基礎與概念整合。

社會學家開始利用圖形來表達組織或群體的社會關係已經有一段時日(Sageman,1994)，在這些圖形中，節點(node)用來表示組織或群體內的成員，邊線(edge)用來表示成員間的連結關係，連結的強度則以邊線的粗細或賦予權重表示，例如溝通的頻率，而節點與邊線爲網路分析的基本要素；並且基於網路的屬性開始開發電腦程式來分析組織或群體的特性，例如成員位於網路的中心性(centrality)是否具有差異，成員的中心性可說是網路分析的重要概念。近年來，研究學者利用開發的軟體並結合有高度運算能力的計算機，從事大型網路的分析，這些網路擁有上千個以上的節點及數以萬計的連結，例如網際網路的視覺化運算(Cheswick and Burch,2000)。

(二)犯罪網路

Bauman 的社會系統論述中指出犯罪的世界是一種社會排除 (social exclusion)的世界。因此，犯罪的組織型式相對的在這個社會排除的小生活世界當中孕生與發展。這些組織成員可以把他們視爲一個網路，犯罪世界如同是社會生活系統的一部份，犯罪組織成員之間所建構的網路關係亦是社會複雜網路結構中的部分組成犯罪成員在犯罪網路之間，透過他們之間所存在的弱聯繫方式來取得犯罪的資訊及建構出其完整的互動通路是維持其組織發展的重要機制。

三、模糊理論[1]

(一)模糊集合運算

在這個部份，關於這篇論文的一些模糊集運算我們做一些回顧。設 A 爲一個離散模糊集合且 A 的表示方式：$A=\{A(a_1)/a_1,\ A(a_2)/a_2,\ldots,\ A(a_n)/a_n\}$,aj 是一個實數而 A(aj)是 aj 的隸屬度，j=1,…,n 且 $0< A(aj) \le 1$ 。

模糊集合 A 是在宇集 X 裡面的一個集合，在模糊集合 A 中所有 x 的所有成員都有一個非 0 的隸屬度，表示方式：$\text{supp}(A)=\{x \in X \mid A(x) > 0\}$。

模糊集合的四種基本運算，包括補集、聯集、交集、和加法做以下的定義(Kaufmann,1985)：

1.模糊集 A 的補集表示寫成 $\bar{A}$ 且 $\bar{A}$ 的隸屬函數寫成 $\bar{A}(x)=1-\bar{A}(x)\ \ \forall x \in X$.

2.模糊集合 A 和 B 的交集表示成 $A \cap B$ ，而 $A \cap B$ 的隸屬函數表示成：

$(A \cap B)(x)=\min[(A(x),B(x))]\ \ \forall x \in X$.

3.模糊集合 A 和 B 的聯集表示成 $A \cup B$ ，而 $A \cup B$ 的隸屬函數表示成：

$(A \cup B)(x)=\max[(A(x),B(x))]\ \ \forall x \in X$.

4.模糊集合 A 和 B 的加法表示成 $A+B$ ，而 $A+B$ 的隸屬函數表示成：

$(A+B)(z)=\max \min[(A(x),B(x))]\ \ \forall x \in X$.

(二) α -割集

設 A 爲模糊集，而 A(x) 爲其歸屬函數，則 ${}^{\alpha}A = \{ x \mid A(x) \ge \alpha \}$ 稱爲 A 的 α -

割集 (α-cuts)；而 ${}^{\alpha+}\mathrm{A} = \{ \mathrm{x} \mid \mathrm{A(x)} > \alpha \}$ 稱爲 A 的α-強割集 (α-strong cut)。

模糊集的割集與強割集均爲傳統集合，它們在將模糊問題轉換成傳統集合問題的過程中扮演著相當重要的角色。模糊集之割集與強割集的基本性質整理如下：

設 A,B 爲模糊集，則 $\forall \alpha, \beta \in [0,1]$ 下列性質成立：

1. ${}^{\alpha+}\mathrm{A} \subseteq {}^{\alpha}\mathrm{A}$；

2.設 $\alpha \leq \beta$ ，則 ${}^{\beta}\mathrm{A} \subseteq {}^{\alpha}\mathrm{A}$ 且 ${}^{\beta+}\mathrm{A} \subseteq {}^{\alpha+}\mathrm{A}$；

3. ${}^{\alpha}(A \cap B) = {}^{\alpha} A \cap {}^{\alpha} B$ 且 ${}^{\alpha}(A \cup B) = {}^{\alpha} A \cup {}^{\alpha} B$;

4. ${}^{\alpha+}(A \cap B) = {}^{\alpha+} A \cap {}^{\alpha+} B$ 且 ${}^{\alpha+}(A \cup B) = {}^{\alpha+} A \cup {}^{\alpha+} B$

設 $A_i, i \in I$ 爲模糊集且 I 爲可數的集合，則

5. $\bigcup_{i\in I}{}^{\alpha} Ai \subseteq {}^{\alpha}(\bigcup_{i\in I} A_i)$ 且 $\bigcap_{i\in I}{}^{\alpha} Ai \subseteq {}^{\alpha}(\bigcap_{i\in I} Ai)$ ；

6. $\bigcup_{i\in I}{}^{\alpha+} Ai \subseteq {}^{\alpha+}(\bigcup_{i\in I} A_i)$ 且 $\bigcap_{i\in I}{}^{\alpha+} Ai \subseteq {}^{\alpha+}(\bigcap_{i\in I} Ai)$ 。

在上述定理中，因爲 I 可能爲無限的集合，所以“$\subseteq$” 與“ $\supseteq$”不可改成等號。若 I 爲有限的集合，則可改成等號。

設 A,B 爲模糊集，則$\forall \alpha \in [0,1]$下列性質成立：

7. $\mathrm{A} \subseteq \mathrm{B} \Leftrightarrow {}^{\alpha}\mathrm{A} \subset {}^{\alpha}\mathrm{B}; \mathrm{A} \subseteq \mathrm{B} \Leftrightarrow {}^{\alpha+}\mathrm{A} \subset {}^{\alpha+}\mathrm{B}$

8. $\mathrm{A} = \mathrm{B} \Leftrightarrow {}^{\alpha}\mathrm{A} = {}^{\alpha}\mathrm{B}$ ；

$A = B \Leftrightarrow {}^{\alpha} A = {}^{\alpha} B; A = B \Leftrightarrow {}^{\alpha+} A = {}^{\alpha+} B$ 。

設 A 爲模糊集，則

1. ${}^{\alpha} A = \bigcap_{\beta<\alpha}{}^{\beta} A = \bigcap_{\beta<\alpha}{}^{\beta+} A$ ；

2. ${}^{\alpha+} A = \bigcap_{\alpha<\beta}{}^{\beta} A = \bigcap_{\alpha<\beta}{}^{\beta+} A$ 。

(三)分解定理

這小節在指出每個模糊集可用所有它的 α-割集或所有它的強割集表示出來，而且表示方法爲唯一。這性質稱爲模糊集的分解。它在說明一個模糊集可看成是一序列的傳統集合。首先，利用每個α-割集可定義另一個模糊集 ${}_{\alpha} A(x) = \alpha \cdot {}^{\alpha} A(x), \forall x \in X$

設 A 爲模糊集，則 $A = \bigcup_{\alpha\in[0,1]}{}_{\alpha} A$ ，式中$\cup$爲模糊集的標準聯集運算。

設 A 爲以 X 爲宇集的模糊集，則

1. $A = \bigcup_{\alpha\in[0,1]}{}^{\alpha+} A$ ；

2. $A = \bigcup_{\alpha\in\Lambda(A)}{}^{\alpha} A$ 。式中 $\Lambda(A) = \{\alpha \mid A(x) = \alpha, x \in X\}$ 爲 A 的水準集。

(四)模糊數

在各種模糊集中，以實數 R 爲宇集的正規模糊集因爲可用以代表模糊數或模糊區間，所以特別重要。例如：在實務上，常會碰到“大約 25”或“大概在 20 到 30 之間

”之類的敘述。這些敘述都可以用模糊數表示，再以模糊理論做相關的推論。一個以實數 R 爲宇集的模糊集 A 要可用以代表模糊數必須滿足下列條件：

1. A 必須是正規模糊集，即 $\sup_{x\in R} A(x)=1$

2. ${}^{\alpha}A$ 必須爲閉區間(Closed intervals)， $\forall\alpha\in(0,1]$

3. ${}^{0+}A$ 必須爲有界(Bounded)。

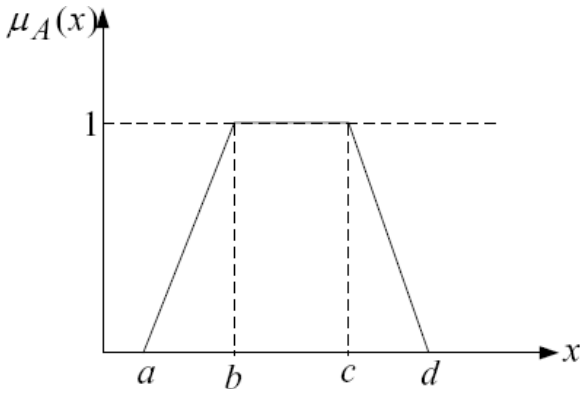
因爲模糊數的 α -割集均爲閉區間，所以模糊數必定爲凸模糊集 (Convex fuzzy set)。但凸模糊集未必是模糊數。

在模糊理論中，最常見的模糊數爲 LR 型模糊數 (LR-type fuzzy number) 與其特例。其中，最常被使用的爲梯形模糊數(Trapezoidal fuzzy number) 與三角模糊數 (Triangular fuzzy number)。其詳細定義如下：

4.梯形模糊數：若模糊集 A 的歸屬函數 μ_A 爲

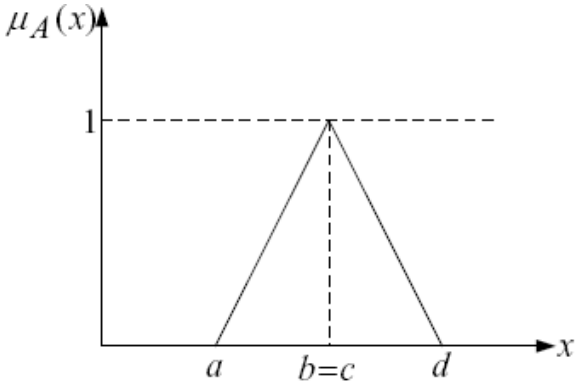
$$\mu_A(x)=\begin{cases}\dfrac{x-a}{b-a}, & a\le x\le b;\\ 1, & b\le x\le c;\\ \dfrac{x-d}{c-d}, & c\le x\le d;\\ 0\text{，其他}\end{cases} \tag{1}$$

則稱爲梯形模糊數，記爲 $A=(a,b,c,d)$。若 $b-a=d-c$ ，則稱之爲等腰梯形模糊數。梯形模糊數之歸屬函數如圖一所示。



圖一:梯型模糊數之歸屬函數

5.三角模糊數：若梯形模糊集 $A=(a,b,c,d)$ 滿足 $b=c$，則稱之爲三角模糊數，記爲 $A=(a,b,d)$。三角模糊數之歸屬函數如圖二所示。若 $b-a=d-c$ 且 $b=c$ ，則稱之爲對稱三角模糊數。



圖二:三角模糊數之歸屬函數

四、犯罪網路之資料萃取與連結分析

(1)資料萃取

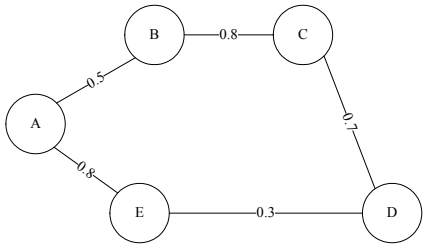
萃取適當資訊，並將這些資訊轉換，以網路圖形來表示。這些資訊是有關實體關聯的原始資料(如電話紀錄、監視日誌及犯罪紀錄)及建構一個網路的表示方式，並且確認哪些在網路中是無相關的實體。現行連結分析在執法實務上主要是由偵查人員針對案件所屬相關資訊手動建立或者利用資料探勘相關軟體來建構連結分析圖形，相當耗時且花費人力。爲了解決犯罪，偵查人員可能要花費大量的時間來從資料庫中作搜尋，閱讀犯罪報告及尋找犯罪者關聯間的線索。製作連結分析圖形，一項不可或缺的工作就是萃取有關個體及龐大原始紀錄相關的資訊並且轉換這些資訊成網路的呈現方式。個體經常被以節點(node)來顯示，並利用網路連接的邊線粗細來表達他們之間相互的關聯強度。一些技術已被開發用來將電腦資料庫中結構式資料紀錄建構成以網路的型態來展現，例如COPLINK Detect是一種基於概念空間的方法，這方法是由Chen及Lynch所發展出來，圖形中的節點代表實體的紀錄(人、組織、車輛、地點)，在這樣的網路中，假如他們一同出現在相同的犯罪事件中，這關聯性將會存在，而且次數或頻率越高，則表示之間的相關性就越強，這種概念空間的方法主要是以統計爲基礎的方法；Goldberg及Senator也建議[27]在金融犯罪的調查期間可以將在交易的資料紀錄以結合及連結的操作來執行，像個人是否有共有的地址、共有的銀行帳號或者相關的交易，這技術已被美國國家司法部所採用用來偵測洗錢的交易及活動。另外，一些其他的技術也能建立網路，這些技術是利用萃取非結構性資料或文字文件，例如偵查人員利用書報文件並依個人習慣繪出案件的連結分析圖形。

(2)連結分析

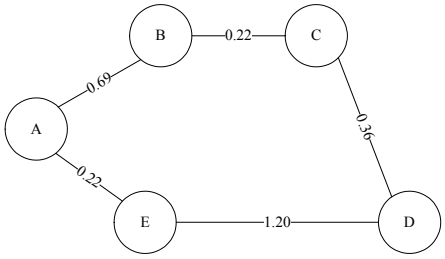
路徑分析，最短路徑演算法是學者經常研究的對象，包括PFS及二元Dijkstra演算法計算出兩節點間的最短路徑，Chen及Lynch也曾提出修改後的PFS演算法，並利用其他演算法與所提出的演算法作效果及效率上的比較分析。

Chen在[5]提出犯罪網路中兩個直接相連的節點關聯性強度是以連結的權重來表示，這權重值將介於0到1之間，並且這權重值可以以機率估算的方式來產生，來顯示兩個節點間的相關程度；一般來說，關聯性強度就是兩個獨立節點間所有通過路徑權重值的乘積，如圖三所示，(A–B–C)乘積爲0.4(0.5*0.8)；(A－B－C－D)是0.28 (0.5*0.8*0.7)

而(A–E–D)是0.24(0.8*0.3)，因此路徑(A–B–C–D)比(A–E–D)有較強的關聯性。然[5]是以最短路徑演算法，來求得最強關聯路徑，而最短路徑以連結權重值加總的方式來進行，並不是以連結權重值乘積的方式，因此必須對原先連結的權重(或稱機率)做數值轉換，因此犯罪網路圖形中的最短路徑，即爲最強關聯路徑，即 W*=-lnW =-ln (Π wi)=-(ln w1+lnw2+lnw3+…+lnwi) 例如(A–B–C–D)經數值轉換後其關聯強度爲，-ln0.28=-ln(0.5*0.8*0.7)=-(ln0.5+ln0.8+ln0.7)=0.05(A–E–D)經數值轉換後其關聯強度爲-ln0.24=-ln(0.8*0.3)=-(ln0.8+ln 0.3)=0.26，轉換後圖形如圖四所示。換言之，圖三是取乘績的最大值，而經數值轉換後，圖四則是取加總的最小值。



圖三:兩個間接相連的節點(節錄自[5])



圖四:經數值轉換後路徑權重之改變

本篇論文利用此數值轉換後的權重爲研究基礎，因此不再於後面各章節作數值轉換之解釋，如表一爲數值轉換的結果。

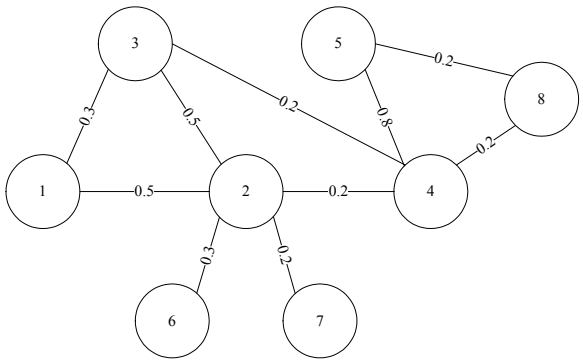
表一:數值轉換表

w	-lnW	W	-lnW
1	**0**	**0.5**	**0.69**
0.9	**0.11**	**0.4**	**0.92**
0.8	**0.22**	**0.3**	**1.20**
0.7	**0.36**	**0.2**	**1.61**
0.6	**0.51**	**0.1**	**2.30**

五、MPFS(Modified Priority First Search)演算法

藉由事先建構好的犯罪網路拓樸找出最佳偵查路徑。假設圖五爲犯罪網路圖形，圖形中各節點與連結內容權重實際上需由實務機關依實際需求做適當之定義。在此我們假

設網路上各節點是理想的(perfect)，可信賴的(reliable)，而節點間之連結是不可信賴的，存有失敗的機率，以這樣的情況來尋找最佳偵查路徑。



圖五:犯罪網路圖形

在現實的情況之下，各節點成員間會因種種因素而使偵查行動被迫於停止，如成員可能被誤認有犯罪行爲、遭受他們之殺害或則長期逃亡而無法掌握其行蹤等等原因，故本文另外也考慮到節點成員之問題並賦予其權重如表二，當然其大小衡量的標準也由實際情況之下做適當的定義。而成本矩陣爲表三。

表二:各節點成員之權重

節點	V1	V2	V3	V4	V5	V6	V7	V8
距離	0.2	0.1	2.3	0.4	0.5	0.6	0.7	0.8

表三:網路犯罪圖形之成本矩陣

	V1	V2	V3	V4	V5	V6	V7	V8
V1	0	0.5	0.3	-	-	-	-	-
V2	0.5	0	0.5	0.2	-	0.3	0.2	-
V3	0.3	0.5	0	0.7	0	1.1	-	-
V4	-	0.2	0.7	0	0.8	1.2	-	0.2
V5	-	-	-	0.8	0	-	-	0.1
V6	-	0.3	-	-	-	0	-	-
V7	-	0.2	-	-	-	-	0	-
V8	-	-	-	0.2	0.1	-	-	0

‘-’代表兩節點無法直接連結，必須透過第三點

假設所要找尋的起點爲節點 V1，終點爲節點 V8。便可以依據犯罪網路圖形進行 MPFS 演算法求出最佳偵查路徑。此時便可得到各節點之來源節點如表四，與起點到圖形中其他點之最短距離如表五。

表四:各節點之來源節點

節點	P[1]	P[2]	P[3]	P[4]	P[5]	P[6]	P[7]	P[8]
距離	--	V1	V1	V2	V8	V2	V2	V4

表五:起點 1 到圖形任何點之最短距離

節點	D[1]	D[2]	D[3]	D[4]	D[5]	D[6]	D[7]	D[8]
距離	0.0	0.5	0.3	0.8	1.5	0.9	0.8	1.4

最後根據表四與表五便可知最佳偵查路徑爲 1－＞2－＞4－＞8 與最短距離爲 1.4。

(一)MPFS 演算法時間複雜度

建構MPFS演算法，因爲一開始即設定起始節點，因此尋找距離起點最近的連結節點複雜度爲$O(N\text{-}1)$，之後要針對U中最小的值做改值的動作，由於自身的節點不用改值，所以複雜度爲$O(N\text{-}2)$，這樣尋找距離最小並且改值的動作總共要做$N\text{-}1$次，所以整個MPFS演算法的複雜度爲$O\left\{n-1\left[\left(n-1\right)+\left(n-2\right)\right]\right\}=O(2n^2\text{-}5n+3)=O(n^2)$。

```
Algorithm MPFS：Search the strongest associated paths in G(V, E)
Input：A set of node V and edge E with weight
Output：Find out the strongest associated Paths by MPFS
s = source node;
d = destination node;
D[v] = distance of a node from the source node;
L[i, j] = network connectivity matrix;
P [v] = predecessor vector;

MPFS ( s,d,L,D )
{
    // Initialize  初始值設定
    Q = {s};                    /* initialize the set of marked nodes */
    K = {};                     /* put next node we can choose */
    D[i] = ∞;                   /* initialize the distance */
    P [v] = 0;                  /* initialize the predecessor vectors */
    L[s, s] = L[d, d] = 0;
    D[v] = d[s->v];             /* Node s connects to V1 and V2 in Graph */
    /* while there are nodes outside Q, and u is not destination */
    while ( Q link other node u )
    {
        for ( u is not in Q )
        {
            choose a node u whose D[u] is minimum//含兩個D[u]相等
```

```
            L'[u,j] = L[u,u] + L[u,j]，j != p[u]
            Q = Q ∪ {u} /* add the closest node to S */
            K = K ∪ {j}
        }
        /* update distance */
        For(u link to j)
        {
            if D[j] > D[u] + L'[u, j]
            {
                D[j] = D[u] + L'[u, j];
                P[j] = u;
            }
        }
    K = K – Q;
}
```

圖六:MPFS 演算法

參、具模糊權數之最佳偵查路徑

本章將犯罪網路圖形之權重值轉換成距離，再利用幾個較好的模糊排序方法來做解模糊，這幾個模糊排序方法在數學上具有良好的代數性質，使得解模糊出來的數值不至於失真太多，最後再利用 MPFS 演算法算出最佳偵查路徑。

一、模糊排序

在現實生活裡，決策者在制定決策時，經常將下屬所提的方案以優劣程度表示，可能將其分成很多指標，而在各個指標上分數較高的評爲優即爲決策者的優先考量方案，然而優的方案比劣的方案優多少，可不可以用一個數字或相對數字來顯示它們的差距，爲了探討這差距，模糊排序變應運而生。

二、模糊排序分類

Lee 與 Li[4]及 McCahone[3]的分類是依模糊可能性的量度與機率的量度(the possibility concept and/or the probability measure) 爲理論基礎，探討模糊數的排序；其分類爲數學方法(mathematical approaches) 及語意方法(linguistic approaches)，數學方法又細分爲可能性理論(possibility theory)與機率性理論(probability theory)。

三、機率性均值與可能性均值

在模糊排序分類中有說到 Lee 與 Li 及 McCahon 的分類是用數學方法，而採用的數學方法中可細分爲機率性理論和可能性理論，而 Dubois and Prade 在早些時間提出了機率性均值，而 Carlsson and Fuller 提出了可能性均值。這兩種均值的共通點就是可以用於解模糊，且具有許多良好的數學性質，而不同點則在於機率性均值並沒有將一個數值出現的高低列爲考慮，而 Carlsson and Fuller 則提出將數值出現的可能性當作權重，

以下爲機率性均值與可能性均值的定義[1]：

(一)機率性均值

有一個模糊數 $\tilde{A}$ ，則 $\tilde{A}$ 的機率性均值 E=[E_ℓ,E_μ]定義爲：

$$E_\ell = \int_{-\infty}^{\infty} x dF^*(x), E_\mu = \int_{-\infty}^{\infty} x dF_*(x) \text{ ；} \quad (2)$$

$$F^*(x) = \sup\{A(r) \big| r \le x\}, F_*(x) = \inf\{A(r) \big| r > x\} \text{ ， } \bar{E} = (E_\ell + E_\mu)/2 \quad (3)$$

稱爲 $\tilde{A}$ 的明確機率性均值。

(二)可能性均值

令 A 爲 LR 型模糊區間，

$$^{\alpha}A = [a_1(\alpha), a_2(\alpha)], \forall \alpha \in [0,1] \text{ ，其 } ^0A = \text{cl}\{z \big| A(z) > 0\} \quad (4)$$

則區間 $M = [M_\ell, M_\mu]$ 稱爲 A 的可能性均值；

$$M_\ell = 2\int_0^1 \alpha\ a_1(\alpha) d\alpha, M_\mu = 2\int_0^1 \alpha\ a_2(\alpha) d\alpha \text{ ，而 } \bar{M} = (M_\ell + M_\mu)/2 \quad (5)$$

稱爲 A 的明確可能性均值。

四、以模糊比序函數解模糊求解犯罪網路拓樸中最佳偵查路徑

有一個無方向性的犯罪網路拓樸，節點和邊上的權重以三角模糊數來表示，執行下列步驟即得到此犯罪網路拓樸上的最佳偵查路徑：

Step1：決定是否將數值出現的可能性視爲權重，決定要使用可能性均值或機率性均值。

Step2：選定一個具有良好代數性質且爲線性函數的模糊排序方法。

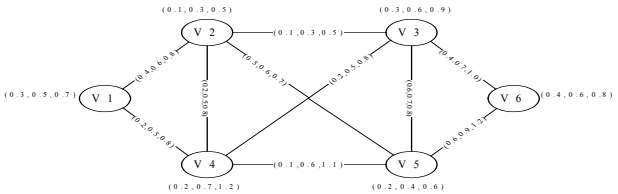
Step3：利用選定的模糊排序方法解模糊以得到一個可以排序的數值。

Step4：將解模糊之後的圖形利用[5]的數值轉換

Step5：利用 MPFS 演算法來求得起點到終點的最短距離，得到最短路徑，此最短路徑即爲犯罪偵查的最佳偵查路徑。

五、數值範例-可能性均值

圖七爲一個具有三角模糊數的犯罪網路拓樸，進行最佳偵查路徑步驟即可找到犯罪偵查的最短路徑：



圖七:具三角模糊數的犯罪網路拓樸

Step1：假設決定使用可能性均值。

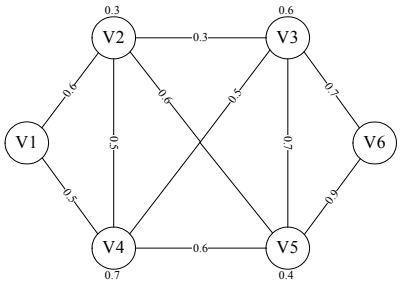
Step2：選定以CM_2^{λ}做爲模糊排序函數。

Step3：在使用CM_2^{λ}這個模糊排序，由上一節得知$\lambda = 0.5$時爲明確的可能性均值，在此以$\lambda = 0.5$當作例子，故其明確的可能性均值爲$\bar{M}(A) = \frac{a + 4b + c}{6}$，使用這條公式當做解模糊的工具。而解模糊的結果如表六所示：

表六:利用CM_2^{λ}解模糊之後各邊的權重

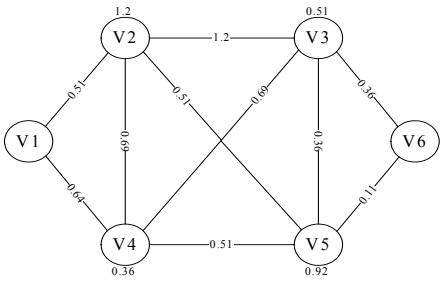
聯結	權數的明確可能性均值
V2	(0.1+4*0.3+0.5)/6=0.3
V3	(0.3+4*0.6+0.9)/6=0.6
V4	(0.2+4*0.7+1.2)/6=0.7
V5	(0.2+4*0.4+0.6)/6=0.4
(s,1)	(0.4+4*0.6+0.8)/6=0.6
(s,3)	(0.2+4*0.5+0.8)/6=0.5
(1,2)	(0.1+4*0.3+0.5)/6=0.3
(1,3)	(0.3+4*0.4+0.5)/6=0.4
(1,4)	(0.5+4*0.6+0.7)/6=0.6
(2,3)	(0.2+4*0.5+0.8)/6=0.5
(2,4)	(0.6+4*0.7+0.8)/6=0.7
(2,t)	(0.4+4*0.7+1.0)/6=0.7
(3,4)	(0.1+4*0.6+1.1)/6=0.6
(4,t)	(0.6+4*0.9+1.2)/6=0.9

而解完模糊其圖形如圖八：



圖八:利用CM_2^{λ}解模糊之後的犯罪網路拓樸

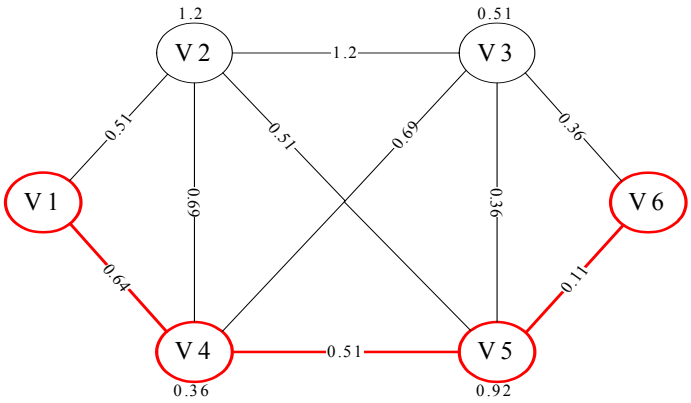
Step 4：將解模糊之後的圖形利用[5]的數值轉換，數值轉換的結果如圖九。



圖九:利用[5]數值轉換之後的犯罪網路拓樸

Step 5：利用 MPFS 演算法來求起點(V1)到終點(V6)的最短距離，以求得最佳偵查路徑：

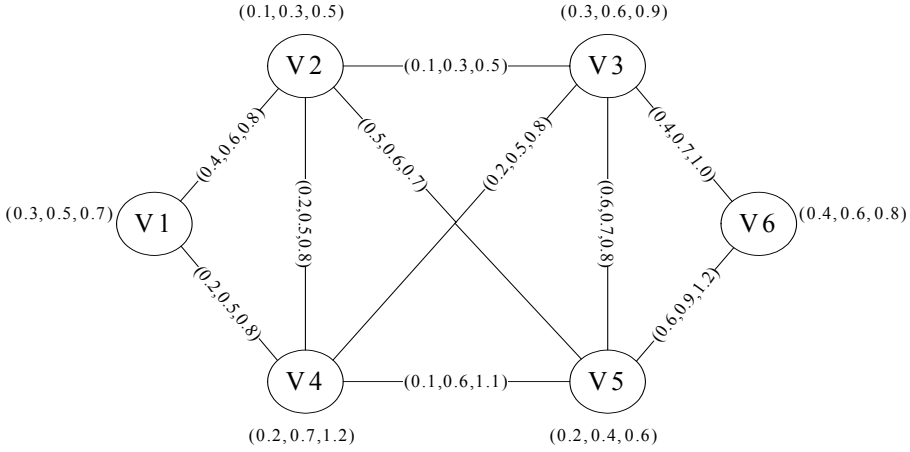
由 MPFS 演算法的執行結果可以知道最強關聯路徑爲 V1→V4→V3→V6，也就是我們的最佳偵查路徑如圖十所示。



圖十:利用 CM_2^{λ} 明確可能性均值解模糊之後的最佳偵查路徑

六、數值範例-機率性均值

圖十一爲一個具有三角模糊數的犯罪網路拓樸，利用最佳偵查路徑步驟的步驟即可找到犯罪偵查的最佳偵查路徑：



圖十一:具三角模糊數的犯罪網路拓樸

Step 1：假設決定使用機率性均值。

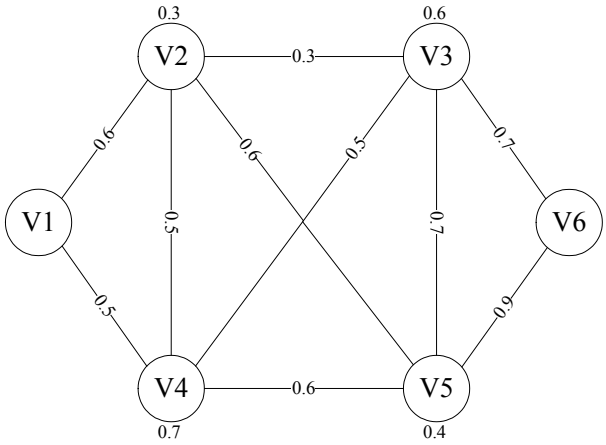
Step 2：選定以FR 做爲模糊排序函數。

Step 3：在使用FR 這個模糊排序，其明確的機率性均值爲 $\bar{M}(A)=\frac{a+2b+c}{4}$ ，使用這條公式當做解模糊的工具。而解模糊的結果如表 4-3 所示：

表七:利用FR 解模糊之後各邊的權重

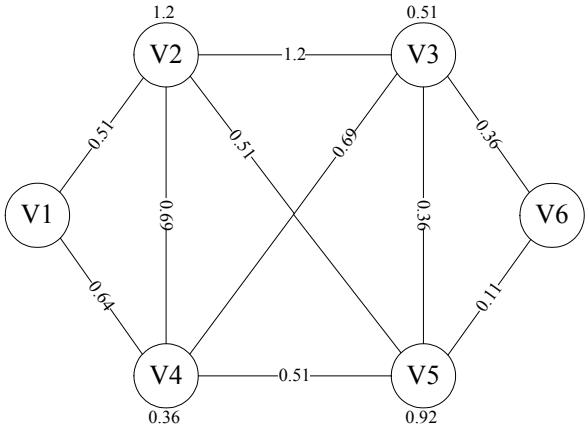
聯結	權數的明確機率性均值
V2	(0.1+2*0.3+0.5)/4=0.3
V3	(0.3+2*0.6+0.9)/4=0.6
V4	(0.2+2*0.7+1.2)/4=0.7
V5	(0.2+2*0.4+0.6)/4=0.4
(s,1)	(0.4+2*0.6+0.8)/4=0.6
(s,3)	(0.2+2*0.5+0.8)/4=0.5
(1,2)	(0.1+2*0.3+0.5)/4=0.3
(1,3)	(0.3+2*0.4+0.5)/4=0.4
(1,4)	(0.5+2*0.6+0.7)/6=0.4
(2,4)	(0.6+2*0.7+0.8)/4=0.7
(2,t)	(0.4+2*0.7+1.0)/4=0.7
(3,2)	(0.2+2*0.5+0.8)/4=0.5
(3,4)	(0.1+2*0.6+1.1)/4=0.6
(4,t)	(0.6+2*0.9+1.2)/4=0.9

而解完模糊其圖形如圖十二所示：



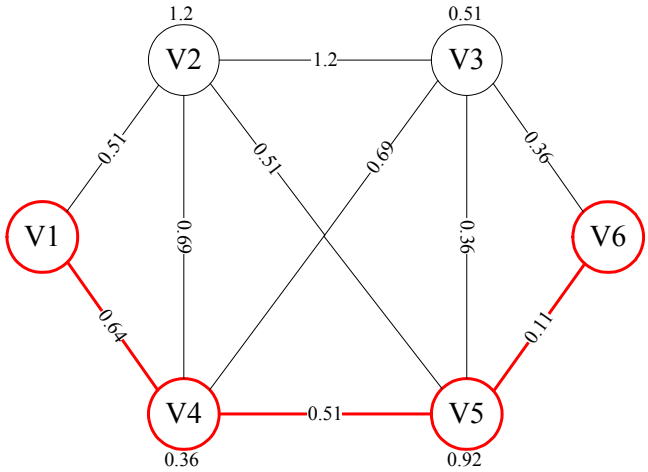
圖十二:利用FR 解模糊之後的犯罪網路拓樸

Step 4：將解模糊之後的圖形利用[5]的數值轉換，數值轉換的結果如圖十三所示。



圖十三:利用[5]數值轉換之後的犯罪網路拓樸

Step 5：利用 MPFS 演算法來求得起點到終點的最短距離，以求得最佳偵查路徑：



圖十四:利用 FR 明確機率性均值解模糊之後的最佳偵查路徑

由 MPFS 演算法的執行結果可以知道最強關聯路徑爲 V1→V4→V3→V6，也就是我們的最佳偵查路徑如圖十四所示。

肆、最佳偵查路徑中的最關鍵邊

在一個犯罪網路拓樸中，我們由前一章的方法找到最佳偵查路徑，但是在偵辦過程中充滿了許多變數，例如：證據被湮滅、犯人潛逃海外等等…，都會使我們的偵查無法繼續下去，但往往前置成本都已經花下去了，不能再從頭開始偵查，因此我們提出一個解決方法讓偵查時能針對偵查路徑中的最關鍵邊先偵查，以爭取犯罪證據的時效性，在犯罪人之間關係消失前先採取偵辦以防需要花更多的成本來尋找替代路徑。最關鍵邊的定義是將某條邊從圖形中移除，所花費的成本爲全部邊中最高的；在這裡我們使用 Malik,Mittal和Gupta[6]所提出的方法。

(一)方法描述

由於在犯罪網路中節點與節點之間的關係，可能是有向邊或者是無向邊，除非有

確切資料才能判別關係是主動還是被動的，若沒有確切資料我們只能假定節點和節點之間是有關係的並以無向邊來表示。我們將一個犯罪網路拓樸分成以起點爲根節點的一棵樹，和以終點爲根節點的一棵樹，當一條最佳偵查路徑(path)從此犯罪網路拓樸中找到，這條路徑是由許多邊(edge)組合而成，爲了爭取犯罪證據消失的時效性，因此一個邊斷掉我們便去找它們斷掉的邊中前後連接的兩個節點，此時斷掉的邊已經將此圖形分成兩棵樹，所以我們就分成三個部份來處理：一個是從起點到斷掉邊的前節點，一個是斷掉邊的替代路徑，一個是從終點到斷掉邊的後節點；將這三段相加與原來最佳偵查路徑權重相差最多的即是最關鍵邊。

(二)最關鍵邊演算法(Most Vital Edge algorithm, MVE)

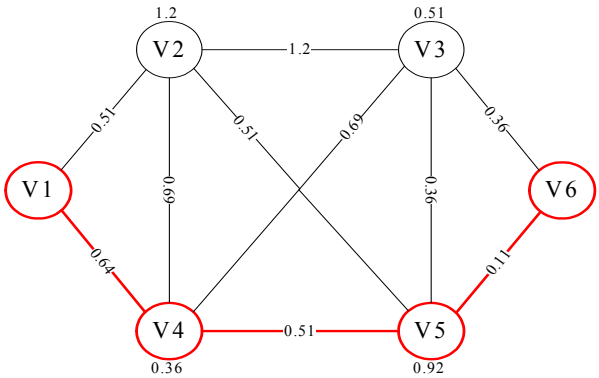
```
Algorithm MVE：Search the most vital edge in the fuzzy shortest path
Input：An fuzzy shortest path
Output: Find out the most vital edge
 m;       // the number of nodes of fuzzy shortest path
 Dist;     //the distance of the fuzzy shortest path from source node to destination
 node
 Dis;       //the array of shortest distance between source node to other nodes
 tempdis; //a variable used to store Dist temporarily
 Main()
 {
    int a,tempdis=0;
    for(i = 2;i <= m-1 ; i++)
    {
              Remove N[i] and connet the N[i]'s edge;
              Call MPFS(s,d,L,Dis);
              Dist=Dis(1,N[i-1])+Dis(N[i-1],N[i+1])+Dis(N[i+1],N[m]);
              If(tempdis < Dist)
              {
                       tempdis=Dist;
                       a = i;       //the most vital point
              }
              Recover N[i] and connet the N[i]'s edge;
     }
 }

Algorithm MPFS：Search the strongest associated paths in G(V, E)
Input：A set of node V and edge E with weight
Output：Find out the strongest associated Paths by MPFS
s = source node;
d = destination node;
Dis[]; /*the array of shortest distance between source node to other nodes*/
L[i, j] = network connectivity matrix;
P [v] = predecessor vector;

MPFS ( s,d,L,Dis )
{     // Initialize 初始值設定
      Q = {s};                    /* initialize the set of marked nodes */
```

```
        K = {};                    /* put next node we can choose */
        Dis[i] = ∞;                /* initialize the distance */
        P [v] = 0;                 /* initialize the predecessor vectors */
        L[s, s] = L[d, d] = 0;
        Dis[v] = d[s->v];          /* Node s connects to V1 and V2 in Graph */
        /* while there are nodes outside Q, and u is not destination */
        while ( Q link other node u )
        {
              for ( u is not in Q )
              {
                   choose a node u whose Dis[u] is minimum//含兩個Dis[u]相等
                 L'[u,j] = L[u,u] + L[u,j]，j != p[u]
                 Q = Q ∪ {u} /* add the closest node to S */
                 K = K ∪ {j}
              }
              /* update distance */
              For(u link to j)
              {
                 if Dis[j] > Dis[u] + L'[u, j]
                 {
                      Dis[j] = Dis[u] + L'[u, j];
                      P[j] = u;
                 }
              }
          K = K – Q;
}
```

圖十五:最關鍵邊演算法

(三)最關鍵邊實例

我們以上述最佳偵查路徑步驟算出的最佳偵查路徑的犯罪網路拓樸當作例子，在此假設其他替代路徑的邊皆爲有效以方便例子解釋：



圖十六利用 FR 明確機率性均值解模糊之後的最佳偵查路徑

由上述最佳偵查路徑步驟我們可以知道V1-V4-V5-V6爲最佳偵查路徑，因此V1-V4、V4-V5、V5-V6即是我們最關鍵邊的候選邊，我們將三個邊分開來討論，最後再與原始最佳偵查路徑比較，總權重相差最多的邊即是最關鍵邊。

第一，首先移除V1-V4，並利用MPFS演算法求得移除V1-V4兩節點之間新的替代路徑，經由MPFS演算法求得V1-V2-V4爲移除V1-V4後最佳的替代路徑且權重加總爲2.4。

因此移除V1-V4後偵查路徑的成本變爲：V1-V4的替代路徑權重加V4-V5的權重加V5-V6的權重=2.4 +0.87+1.03=4.3。

第二，接著移除V4-V5，並利用MPFS演算法求得移除V4-V5兩節點之間新的替代路徑，經由MPFS演算法求得V4-V3-V5爲移除V4-V3後最佳的替代路徑且權重加總爲1.56。因此移除V4-V3後偵查路徑的成本變爲：V1-V4的權重加V4-V5的替代路徑權重加V5-V6的權重=1+1.56+1.03=3.59。

第三，接著移除V5-V6，並利用MPFS演算法求得移除V5-V6兩節點之間新的替代路徑，經由MPFS演算法求得V5-V3-V6爲移除V5-V6後最佳的替代路徑且權重加總爲1.23。因此移除V5-V6後偵查路徑得成本變爲：V1-V4的權重加V4-V5的權重加V5-V6的替代路徑=1+1.43+1.23=3.66

V1-V4移除後權重總和與原來最佳的偵查路徑相差最大，因此V1-V4爲我們的最關鍵邊。

(四)時間複雜度

依照最關鍵邊演算法要將整個圖形中最佳偵查路徑中的每一個邊都要走訪一次，時間複雜度爲$O(m-1)$，移除一條邊所需要花的時間複雜度爲$O(1)$，之後呼叫MPFS演算法來尋找兩點之間替代路徑的權重，整個尋找過程中時間複雜度爲$O(N^2)$，接著將原本固定的路徑與替代路徑相加，時間複雜度爲$O(m-1)$，之後判斷哪一個移除後的總權重爲最大，此邊即爲最關鍵邊，判斷的複雜度爲$O(m-2)$，最後將移除的邊回復，複雜度爲$O(1)$，因此整個演算法的時間度爲$O(m-1)(N^2+2m-1)=O(mN^2+m^2)$。

伍、結論

最短路徑問題在現實生活中有著廣泛運用，在最短路徑的規劃方面，一般都是找實際上最短的爲最關鍵路徑，但現實情況可能並非如此，網路模型中之節點可能也是不可信賴的，有失敗的機會存在，例如說：我要找一個嫌犯，憑著專業的判斷知道如何以最少的資源和人力來循線逮捕，但事與願違，這個成員可能被誤人爲有犯罪行爲，遭受其他犯罪組織謀殺，或者長期潛逃海外等，這將使得最強關鍵路徑失效，並且導致後續的偵查行動中斷。因此本文提出一個以模糊數學的架構，讓每一個邊和節點都賦予一個隸屬度，將不可靠的邊和節點賦予較低的隸屬度；相對的，將較有可能的路徑賦予較高的隸屬度，藉由模糊數學的運算方式來找出最短的路徑，使這條路徑將比實際上最短的路徑更具有彈性。

參考文獻

[1]鄧凱年，“具模糊權數之最小生成樹問題”，*碩士學位論文，南台科技大學，工業管理研究所*，2006：頁9-21。

[2]張恆睿，“應用社會網路分析於犯罪網路模型之研究”，*碩士學位論文，中央警察大學，資訊管理研究所*，2006：頁17-28。

[3]C. McCahone, “Fuzzy set theory applied to production and inventory control”, *Ph.D. Thesis, Department of Industrial Engineering, Kansas State University*, 1987

[4]E.S. Lee and R.J. Li, “Comparison of fuzzy numbers based on the probability measure of fuzzy events”, *Computers and Mathematics with Applications 15*, 1988: pp.887-896.

[5]Jennifer J. Xu and Hsinchun Chen, “Fighting organized crimes: using shortest-path algorithms to identify associations in criminal networks”, *Department of Management Information Systems, University of Arizona, Tucson, AZ 85721, USA*, 2004: pp.477-481.

[6]K. Malik, A.K. Mittal and S.K. Gupta, “The k most vital arcs in the shortest path problem”, *Operations Research Letters 8*, 1989: pp.223-227.

[7]Scott J M., “Organized Crime: A Social Network Approach”, *Crime, Law and Social Change*, 2000: pp.301-323.