國立交通大學

資訊科學與工程研究所

碩 士 論 文

在動態路徑導航中威脅車輛對車輛行駛效率之影響

The Influence of Threat Vehicles on Dynamic Navigation in Vehicular Ad Hoc Network

研 究 生：陳柏志

指導教授：孫春在　教授

中 華 民 國　九 十 九 年 六 月

在動態路徑導航中威脅車輛對車輛行駛效率之影響

The Influence of Threat Vehicles on Dynamic Navigation in Vehicular Ad Hoc Network

研 究 生：陳柏志　　Student：Po-Chih Chang

指導教授：孫春在　　Advisor：Chuen-Tsai Sun

國 立 交 通 大 學

資 訊 科 學 與 工 程 研 究 所

碩 士 論 文

A Thesis

Submitted to Institute of Computer Science and Engineering

College of Computer Science

National Chiao Tung University

in partial Fulfillment of the Requirements

for the Degree of

Master

in

Computer Science

June 2010

Hsinchu, Taiwan, Republic of China

中華民國九十九年六月

在動態路徑導航中威脅車輛對車輛行駛效率之影響

學生：陳柏志　　指導教授：孫春在 教授

國立交通大學

資訊科學與工程研究所

摘要

由於車用隨意網路(Vehicular Ad hoc Network, VANET)的發展，駕駛人能夠透過車載機和路側裝置，進行交通資訊的蒐集與傳播的工作。動態路徑導航就是以車用無線網路為基礎，透過車間通訊彙集並整合路況資訊，得到最即時且動態的路況資訊。由於在VANET中各車輛處於寡勝賽局，可能出現以私利考量為優先的威脅車輛，將會對其它車輛造成極大影響。目前對威脅車輛尚未發展出完美的驗證方法，故本研究藉由在動態路徑導航系統中加入威脅車輛，觀察威脅車輛的影響並尋求解決方法。

本研究透過車間通訊蒐集並整合路況資訊，獲得最即時的訊息，進而使用路徑導航系統找出最短時間路線並往目的地前進。本研究在此基礎模型中加入了三種威脅車輛：a. 偽造路況、b. 偽造路況和時戳、以及c. 考慮惡意訊息回向。在路況更新方法方面，除了基本的最新時戳法則和加權時戳法則這兩種方法外，還加入了考慮地理相對位置的兩種路況更新方法。

研究結果顯示，考慮惡意訊息回向的威脅車輛對網路影響最大；考慮地理位

置和加權時戳法則的路況更新方法能有效抵抗威脅車輛的干擾；加權時戳法則的路況更新方法多跑的距離會比較少；而考慮地理位置和最新時戳法則的路況更新方法在擁塞度方面表現最佳。

關鍵字：車用隨意網路、車間通訊、威脅模型、動態路徑導航

The Influence of Threat Vehicles on Dynamic Navigation in Vehicular Ad Hoc Network

Student：Po-Chih Chen Advisor：Dr. Chuen-Tsai Sun

Institute of Computer and Information Science

National Chiao-Tung University

ABSTRACT

With the development of vehicular ad-hoc network (VANET), drivers can use on-board unit (OBU) to share traffic information via inter-vehicle communication (IVC) or roadside-to-vehicle communication (RVC). Through the dynamic navigation, a route-planning system based on real-time information sharing, drivers can find smooth paths to their destinations immediately.

Because of the property of the minority game in VANET, the threatening vehicles might jam traffic operations on purpose for their personal benefit. Desirable faultless validation methods for detecting such threatening vehicles have not been completely developed yet, so in this study we try to find solutions by putting threatening vehicles into the dynamic navigation model.

In this study we build a dynamic navigation traffic model, and then propose schemes for handling three kinds of threatening vehicle: the weight-modified scheme, the weight-modified and timestamp-modified scheme, and the evil message-reverberated scheme. In addition to the basic traffic information sharing methods, we also propose a new traffic information sharing method that takes the

relative vehicle locations into consideration.

Experimental results show that the evil message-reverberated scheme demonstrate much bigger influence to VANET than the other two types. Our results also show that the traffic information update method with relative vehicle location is helpful in resisting the interference of threatening vehicles; the weighted update method can avoid unnecessary movement; and the timestamp-first update method with relative vehicle location has the best performance in terms of comfortable driving.

Keywords: VANET, Inter-Vehicle Communication, Threat model, Dynamic Navigation

誌謝

轉眼間兩年的碩士生活就要畫下句點，回想剛進交通大學時，第一次要來北部生活的不適應，以及從實習老師轉換身份成學生，心理滿是惶恐與害怕，還好孫老師和實驗室同學們都很照顧我，讓我很快適應這邊的生活。

在眾多人的幫助下，終於完成了這一份論文。首先要感謝孫老師兩年來的指導，還有崇源學長這一年多來的幫助，每當我遇到問題時都會很有耐心的幫助我解決。也要感謝我的口試委員曾憲雄教授、胡毓志教授和陳穎平教授，不僅細心的幫我發現名詞的誤用，也給了我不少意見與改進的方向，讓我的論文能更加的完善。

另外我也要感謝博士班學長，宇軒、聖文、宜睿、王豪、基成和立先在這段期間給我論文上的建議。還要謝謝 97 級的大家，謝謝大家這兩年來對我的包容和照顧，在我失落時給我很多鼓勵。尤其要感謝一起作車用無線網路這塊領域的泰源，在這段時間對我的幫助，也讓我不用在這塊陌生的領域中孤軍奮戰。當然也要感謝實驗室的學弟妹，在口試當天的物品準備給予的幫助，讓我們不用擔心瑣碎事情，能夠全心準備口試。

最後，我要把這份喜悅跟榮耀獻給我最親愛的父母親，謝謝你們讓我求學之路可以無後顧之憂的念上來，在寒流來時還特地北上拿厚的衣物給我，讓我真的非常的感動，很感謝你們無怨無悔的付出。

目錄

表目錄

圖目錄

第一章　緒論

1.1 研究背景和動機

近幾十年，由於車輛成長的速度驚人，加上道路容量無法大規模的增加，世界各國主要城市的交通堵塞狀況持續惡化。將電腦和通訊科技結合並且運用在運輸系統，藉以提升運輸系統效能已經是各個國家努力的目標，而這種發展可以統稱為智慧型運輸系統(Intelligent Transportation System, ITS)。

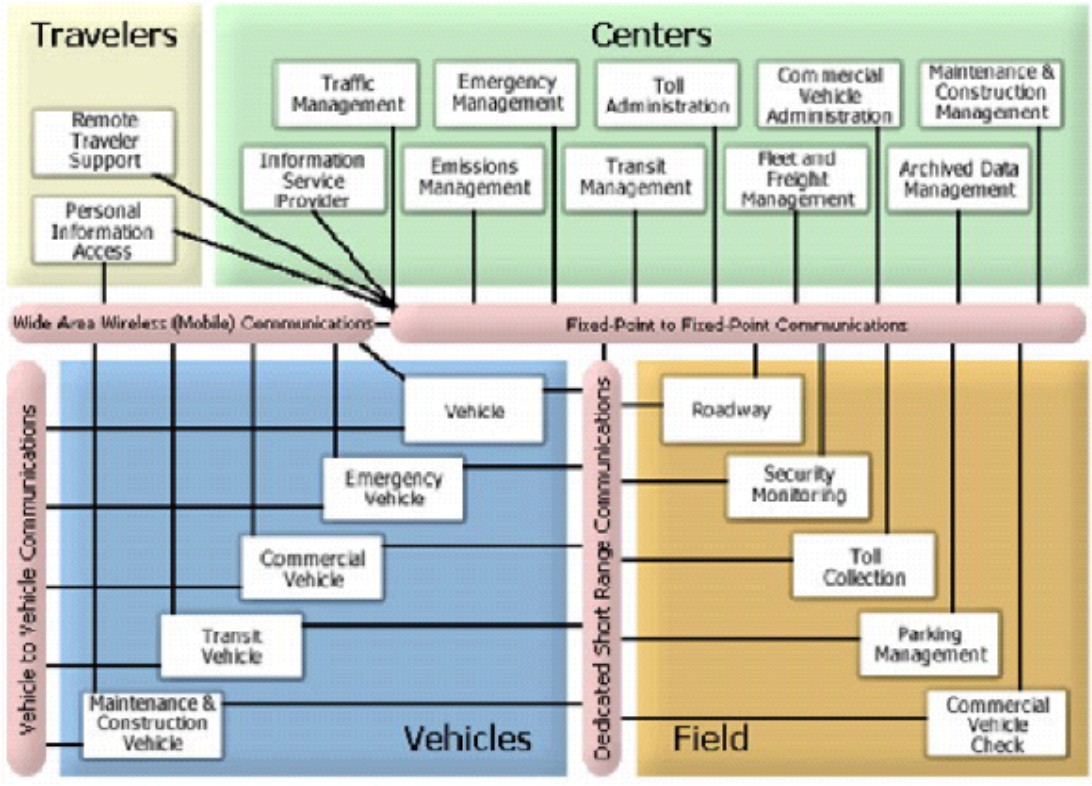


圖 1.1 ITS 基礎架構圖
資料來源：U.S. GAO(1997)

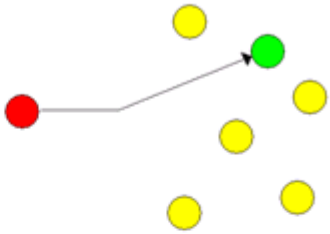
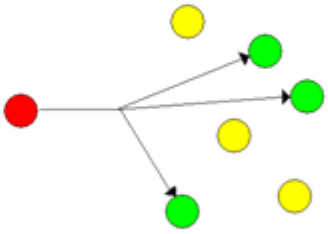
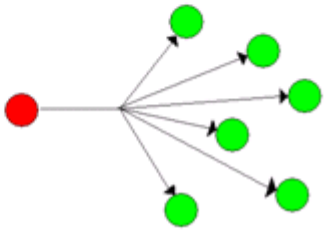
圖 1.1 為 ITS 的基礎架構圖。人們藉由在車輛上安裝車載機(On Board Unit, OBU)，車輛間得以互傳訊息；車輛也可以透過 OBU 和路側裝備(Roadside Unit, RSU)進行資訊交換；RSU 可以透過實體網路線路將接收到的資訊傳送到控管中

心，控管中心也可以將要散佈到路網中的資訊透過 RSU 傳送給道路上的車輛。從上述可以將 ITS 中訊息交換的行為分為車間通訊(Inter-Vehicle Communications, IVC)、車路通訊(Roadside-to-Vehicle Communications, RVC)以及混合 RVC 及 IVC 等等三種。

IVC 指的是車輛在可傳輸範圍內，透過 OBU 在無線網路的環境中與其它車輛相互傳遞訊息；RVC 主要是透過 OBU 和 RSU 進行資訊交換。兩者的差別，在於 RVC 需要透過控管中心進行資訊的整合，再透過 RSU 將整合過的道路資訊傳送給道路上的車輛；而 IVC 不需透過整合的資訊服務中心，只需透過 OBU 蒐集其它車輛的資訊，並將資訊經由彙整後呈現給駕駛人。IVC 獲得的道路資訊會比 RVC 獲得的道路資訊更加即時。

IVC 資訊的擴散與傳送封包的方法息息相關。車輛往往會將訊息傳送到很遠的地方，但無法在一次的封包傳遞中就到達目的地，故會以多次跳躍(multi-hop)的形式來進行資訊的散佈。在傳遞訊息的過程中，擴散的資訊量會依照接收封包的車輛數提高而提升。如表 1.1，根據接收封包車輛數的不同，可以分為單點傳輸(unicast)、多點傳輸(multicast)和廣播(broadcast)這三種路由模式。三種路由模式都有相同的通訊範圍，不同的封包接收車輛數。在本研究中，需要足夠多的路況資訊來進行路況整合，故會以廣播的路由模式傳遞資訊。

表 1.1 資訊散佈路由模式

路由模式	圖示
單點傳輸 (unicast)	
多點傳輸 (multicast)	
廣播 (broadcast)	

在 ITS 中通訊所使用的無線通訊方式，大部分的節點都是由移動的主機所構成，所以稱為行動式隨意網路(Mobile Ad Hoc Network , MANET)。車輛與車輛或是車輛與 RSU 在 MANET 網路環境中通訊又稱為車用隨意網路(Vehicular Ad Hoc Network, VANET)，由 RVC 和 IVC 所組成的 VANET 是 MANET 中一種快速發展的型態 (Blum, Eskandarian, & Hoffman, 2004; Biswas, Tatchikou, & Dion, 2006)。

MANET 和 VANET 之間有許多的不同點。例如：在 VANET 中車速遠大於 MANET 上的節點、VANET 比 MANET 更容易形成高度動態的環境等等。為了因應在 VANET 中高速行駛的通訊狀況，在 2004 年以具有無線通訊能力的 IEEE 802.11a 為通訊技術基礎，制定了 IEEE 802.11p 通訊標準，有效的應用在高速移

動上。

VANET 的發展提供了許多的應用，其中關於安全性的研究是一種重要的應用。 (Abolhasan, Wysocki, & Dutkiewicz, 2004; Bernsen & Manivannan, 2009)研究並且比較不同的封包繞送協定，探討如何透過 VANET 傳送即時的路況資訊封包，能夠使封包傳的更快且可靠性更高，可以讓車禍或是緊急事件的訊息封包快速傳遞且有效的讓其他駕駛者知道。Tang & Yip (2010)透過接收車況的資訊封包，得知附近車輛的車速、車距、行駛方向等等，經由時間分析產生碰撞警告，有效的提高駕駛者行車安全。Chang, Tsai, & Young (2010)在車上安裝感測器，透過偵測附近車輛的車況，藉此預測出碰撞的產生。上述的研究，有效的提高行車的安全。

車輛導航系統也是一種重要的應用服務。根據使用的資訊傳遞方法不同，可以分為集中式系統和分散式系統 (Ohara, Nojima, & Ishibuchi, 2007; Zhao & Cao, 2008; Kitani, Shinkawa, Shibata, Yasumoto, Ito, & Higashino, 2008)。集中式系統透過在路邊設置許多偵測器，將路況資訊傳送給交通控管中心，經過彙整分析之後，再透過 FM 廣播、網頁或是 RVC 等方式傳送給駕駛者；分散式系統假設車輛有安裝 OBU，車輛透過 IVC 的方式收集路況資訊，經過 OBU 整合資訊並呈現給駕駛者。可是集中式系統的偵測器價格昂貴又不易維修，且需要配置實體網路線路，才能將資訊傳回交通控管中心，因為成本高，因此只有在重要的道路上才有設置；加上路況資訊需要經過交通控管中心整合才會傳送給駕駛者，交通資訊並不即時。相對的分散式系統只需安裝 OBU，即可透過 IVC 交換資訊，和集中式系統相比，建構的成本低且即時。

可是惡意攻擊會對道路安全造成危害 (Yan, Olariu, & Weigle, 2008)。如惡意修改緊急訊息，使得後方車輛以為前方車況良好，卻不知發生重大車禍或是突發狀況等等，造成嚴重的道路壅塞。或是發送偽造的訊息，如虛擬車輛的封包，讓

駕駛者誤判前方有車輛存在而緊急煞車，進而造成重大車禍。

Lin, Sun, & Shen (2007)和 Yan, Olariu, & Weigle (2008)在個別的研究中，對 VANET 中的威脅模型作出整理。其中使用 IVC 的威脅模型有下列幾種：

1、 偽造訊息攻擊(Bogus information attack)：攻擊者為了某些目的傳送偽造的訊息。例如，Sybil 攻擊 (Douceur, 2002)，攻擊者發送多個偽造的身份，讓其它車輛產生幻覺，造成車禍的發生。或如 Leinmuller, Schoch, Kargl, & Maihofer (2005)提出錯誤位置攻擊，威脅車輛透過偽造自身位置，進而攔截路上的所有資訊。

2、 訊息重送攻擊(Message replay attack)：攻擊者可能在某些時刻重送正確的封包，進而擾亂交通。

3、 訊息修改攻擊(Message modification attack)：攻擊者收到封包後，修改訊息內容。例如，車禍所發出的緊急訊息，修改其對緊急事件的估計值，降低其他駕駛者的戒備。

4、 偽裝身份攻擊(Impersonation attack)：攻擊者可能偽裝成其他車輛。

5、 阻斷服務攻擊(Denial-of-service attack) (Garg & Reddy, 2004)：攻擊者可能傳送大量不相關的訊息，佔用頻寬和消耗其他車輛的計算資源。

其中，Leinmuller, Schoch, Kargl, & Maihofer (2005)提出的威脅模型，封包的成功傳送率下降了 50%。隔年，Leinmuller, Schoch, & Kargl (2006)提出了一個竊聽的破解方法，利用車輛可以在自身傳輸範圍內進行竊聽的行為，進一步的偵測到威脅車輛的存在，在這個破解方法下，成功傳送率可以高達 95%。

Yan et al.在研究中提到，在某些情況下，破解方法還是偵測不到威脅車輛的存在。例如：當車輛前後被其它車輛平行遮擋到，無法使用雷達時，如果區域中心的車輛剛好是威脅車輛的話，即使威脅車輛刪除封包或是修改封包訊息，還是無法被偵測到。雖然從宏觀的觀點來看，這種無法偵測到的威脅車輛可以被忽略掉，可是當這種威脅車輛一多，是否會造成整個網路的紊亂。

在車間通訊中，除了威脅模型的攻擊之外，也會有其他非惡意的現象造成車輛混淆。例如，在高速公路的某個路段，可能出現壅塞的現象，卻看到投機取巧的駕駛者行駛路肩，使得自身的訊息封包相對於其他的車輛，在車速上顯得非常突兀。或者車載機的程式發生錯誤，在收到封包之後，進而修改封包內容，造成路徑規劃受到影響；甚至是不會發送收到的訊息，如果剛好形成訊息傳送的斷層，也可能影響其他駕駛者對路況的判斷。上述的這些狀況，都稱為無意的攻擊行為。

公共利益(publice good)和私人利益(private interest)的理論常引起社會學家、經濟學者和生態學者的興趣，它可以被表示成數學上簡單卻很難分析的模型，例如知名的囚犯困境問題 (Poundstone, 1992)。在我們的研究中，從公利和私益的角度來看。車輛間彼此分享資訊，透過共同合作的方式，可以讓駕駛者有較佳的路況資訊。可是這種共存共容的場景，卻可能遭有心人的利用。例如：製作導航系統的公司為了讓用戶有更好的行車路況，因而透過發送偽造的封包訊息，將其它車輛導向其餘路段，進而讓用戶有更好的行車路況。威脅車輛在其它車輛都合作的狀態下，透過背叛他人，使自己有最佳的行車路況。當互相背叛的情形發生，互相傳送偽造的路況資訊，反而使得大家對行車路徑都做出錯誤的判斷。

從以往的研究來看，大多數人都集中在 ITS 中 IVC 的應用上，某些基於這些應用的標準也陸續被研究使用，如 IEEE 802.11p。也有些研究專注於 VANET

環境中的威脅模型。但是結合這兩個領域的相關研究卻很少。

本論文結合了路徑導航和威脅模型，並在這個模型中研究威脅車輛的容忍度分析。如圖 1.2，系統中的車輛可以為了有良好的行車路況，可以修改自身的路況資訊並發送給其它車輛，造成前車的轉向，使自己有更好的行車路況。

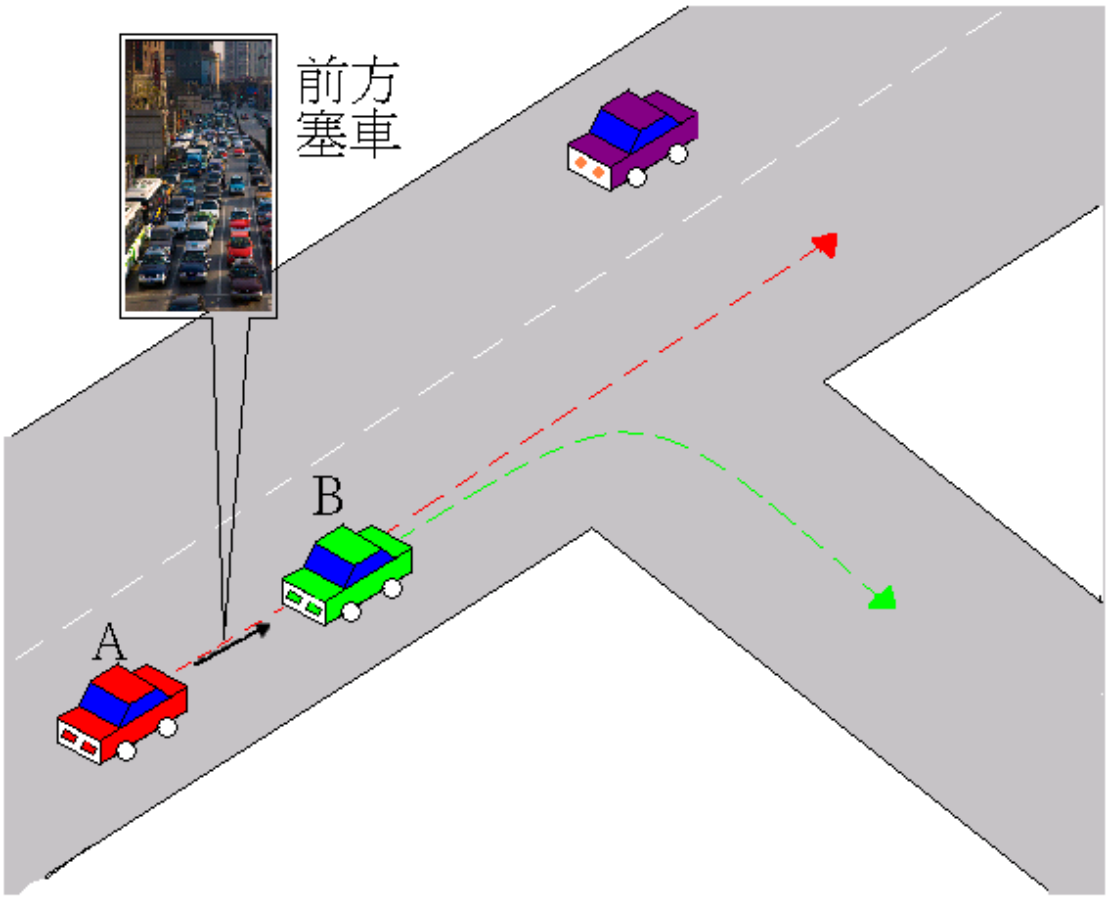


圖 1.2 偽造訊息攻擊

1.2 研究目標

本論文的目標在於針對路徑導航系統結合威脅車輛的模型，在不同的威脅車輛種類下，利用不同的路況更新方法，觀察在不同的車輛密度和不同的威脅車輛比例下，整體路網惡意封包訊息的比例以及正常車輛效能。

本研究想要釐清在各種狀況下，哪種路況資訊的更新方法較佳。亦即從系統

的角度，觀察哪種路況更新方法能有效的抵抗威脅車輛的干擾；在各種環境下，哪種路況更新方法能讓車輛效能較佳。

依據上面所說的目標，我們使用 C 語言去開發模擬系統，在系統中，建構了網狀的路網、基本的車輛移動模型、動態的車輛網路鄰居拓樸，以及網路層廣播封包的發送，系統中的每台車輛都可以利用 OBU 將收到的廣播封包的資訊，拿來做路況資訊的更新，再根據新的路況資訊作路徑規劃。以上，一個動態路徑導航系統完成。

我們建立了一動態路徑導航系統。本研究要探討的是在任何情況下，正常車輛在不同路況更新方法下的效能關係，所以我們會在導航系統中加入威脅車輛，並根據囚犯困境理論，假設駕駛人會尋求自身最大的利益，來支持威脅車輛的存在。

有了結合動態路徑導航系統和威脅車輛的模型，最後我們要做的就是去探討威脅車輛的容忍度分析。在各種情況下，使用不同的路況資訊更新方式，去比較各種路況資訊更新方式在何種情況下能有效抵抗網路中的惡意訊息；並比較哪種路況資訊更新方式能有較佳的效能。最後再觀察所得到的曲線和數據，為得到的現象做出合理的解釋。

綜合上述所說，我們建構了一個動態路徑導航系統，並結合了威脅車輛，透過模擬實驗以及參數的調整，對得到的結果提出合理的說明。

1.3 研究重要性

從駕駛者的角度，開車時比較在乎是否能少走一點距離和是否擁塞。在本研究中，即使路網中有威脅車輛存在，意圖擾亂交通，透過模擬的方法可以找出在

不同路網密度中，哪種路況更新方法可以讓駕駛者多跑的距離變少，使其更省油；也可以找出哪種路況更新方法可以讓駕駛者行車不會擁塞。從使用者的意願，可以自行選擇使用何種路況更新的方法，來達成自己偏重的喜好。

對汽車導航業者來說，導航系統是否能普遍的被使用者所使用，不外乎是導航系統所給的規劃路線是否真的能給予最佳的路徑。可是目前的動態導航系統只能應付路上車輛都是正常車輛的狀況。一旦路網出現威脅車輛，目前的導航系統能否有效的抵擋威脅車輛帶來的干擾，還是個未知數。本研究提供了在不同威脅車輛種類，各種路網狀況下，四種路況更新方法效能的比較，對於導航系統設計師，可以在設計導航系統時考慮我們所模擬出的結果。

1.4 研究問題

傳統的路徑導航系統，會隨著人數使用的增加，使得到同一目的地的車輛一多，反而造成行車路況的不佳，為了解決這個問題，可以即時更新路況資訊的動態路徑導航系統陸續被提出。

在這邊我們要研究的是，當動態路徑導航系統結合威脅模型之後，在各種情況下，隨著威脅車輛比例增加，哪種威脅車輛對網路造成的影響最大，哪種路況更新方法可以有效抵抗威脅車輛的干擾，還有不同路況更新方法對效能的會有怎樣的變化。

當動態路徑導航系統和威脅車輛相結合，為了對威脅車輛作容忍度分析，我們提了三種路況更新的方法：最新時戳法則、加權時戳法則和考慮地理位置優先。並且藉由調整路網密度和威脅車輛比例，去做模擬實驗。綜合上述所說，可以把我們要研究的問題條列如下：

1、 在動態路徑導航系統結合威脅車輛的模型，探討哪種威脅車輛模型對網路影響最大。

2、 探討哪種路況更新方法最能有效抵抗威脅車輛的影響。

3、 透過調整路網密度和威脅車輛比例這兩個參數，比較四種路況更新方法，哪種方法的效能會比較好。

第二章 文獻探討

在本章節中的第一節，會介紹車用無線網路的一些基本架構和應用；接著第二節介紹典型的囚犯困境及其一般表示形式；然後第三節會說明 VANET 中封包廣播的一些傳播機制；第四節將會介紹目前在 VANET 中的威脅模型。

2.1 車用無線網路（Vehicular Ad Hoc Network, VANET）

在本節中，會詳細的介紹 VANET 中相關的研究。第一小節會先說明 VANET 和 MANET 的差異，第二小節將介紹 VANET 所使用的 IEEE 802.11p 通訊標準，第三小節會介紹 VANET 的網路架構，第四小節會介紹 VANET 中相關的應用，最後一小節會說明在 VANET 中的節點移動模式。

2.1.1 VANET 與 MANET 的差異

目前在車間通訊所使用的無線通訊方式是 Ad Hoc。在 Ad Hoc 網路中大部分的節點都是由移動的主機所構成，又稱為 MANET(Mobile Ad Hoc Network)。在 VANET(Vehicular Ad Hoc Network)環境中，每一個節點即是以車輛為單位在 MANET 的環境中進行無線通訊。

VANET 與 MANET 之間有以下幾點不同的特性：

1. 動態且快速變動的網路拓樸：因為在 VANET 中的節點是可移動的車輛，即使 MANET 中的節點也具有移動的特性，其移動速度和 VANET 相比還是慢很多。高速移動相對的網路拓樸會呈現動態且快速的變化，因此在 VANET 的環境中傳遞資料也會相對的困難許多。

2. 可預測的路徑：在 MANET 中的節點可以隨意移動，無法有效的預測其行徑路線。而在 VANET 中的節點雖然移動速度快，但受限於道路的特性，只能沿著道路的分佈而移動，因此，可以使用電子地圖或其它預測工具，有效的預測節點的移動方向和路線。

3. 網路連線的維持困難：在 MANET 的環境中，一個可移動的節點一旦脫離了閘道器的涵蓋範圍，或是欲傳輸的目標節點不在傳送範圍內，就會造成斷線。在 VANET 中，由於節點的移動速度快，這種情形更常發生。

2.1.2 IEEE 802.11a 和 802.11p

802.11a 在 1999 年獲得批准，是 802.11 原始標準的一個修訂標準。802.11a 與原始標準採用了相同的核心協議。具有兩個特性使得 802.11a 適用於車間通訊：(1)、由於 2.4GHz 的頻帶已經被廣泛使用，所以使用 802.11a 具有較少衝突的優點。(2)、由於 802.11a 使用了高載波頻率，所以傳輸距離無法像 802.11b 和 802.11g 那般遠，但用於車間通訊這種短距通訊已經足夠。

IEEE 802.11p(WAVE：Wireless Access in the Vehicular Environment)標準採用 5.9GHz 頻段，利用 802.11a 作為通訊技術。具有兩項特性：

1. 與其它規格互通：為了避免市場接受度受到影響，IEEE 802.11p 除了與 ASTM E2213-03 相容，還和 TC204 WG16(ISO 組織中專門制定車用規格的單位)取得協議，其將支援 IEEE 802.11p 的最終版本。因此未來在佈建與使用上，將具有較經濟的效果。

2. 使 IEEE 802.11a 可應用於高速移動：IEEE 802.11a 雖然可支援 54 Mbps 的傳輸速度，但無法應用在高速移動。IEEE 802.11p 對 IEEE 802.11a 作

部分修正，使其可應用於高速移動下。

2.1.3 VANET 的網路架構

在 VANET 環境中，結合 IVC 和 RVC 會形成一個 VANET 網路，而 VANET 網路架構可以區分為以下三種：

- 車路通訊(Roadside-to-Vehicle Communications, RVC) (Korkmaz, Ekici, Ozguner, & Ozguner, 2004)

如圖 2.1 所示，路側裝置(Road-Side Unit, RSU)在這邊扮演車輛和外部網路的閘道器。移動的車輛透過 RSU 可以連接到外部網路，也能透過 RSU 接收到外部網路發送進來的相關資訊；而 RSU 也可在本身的可傳輸範圍內傳遞資訊，只要在 RSU 可傳輸範圍內的車輛都可以接收到資訊，通常用於前方路況通知或是廣告資訊。

但在 RVC 的架構下，因為車輛具有移動的特性，所以一旦車輛離開了 RSU 的傳輸範圍，便會使車輛和 RSU 先前建立好的路由路徑斷裂，造成傳輸的資訊失敗。

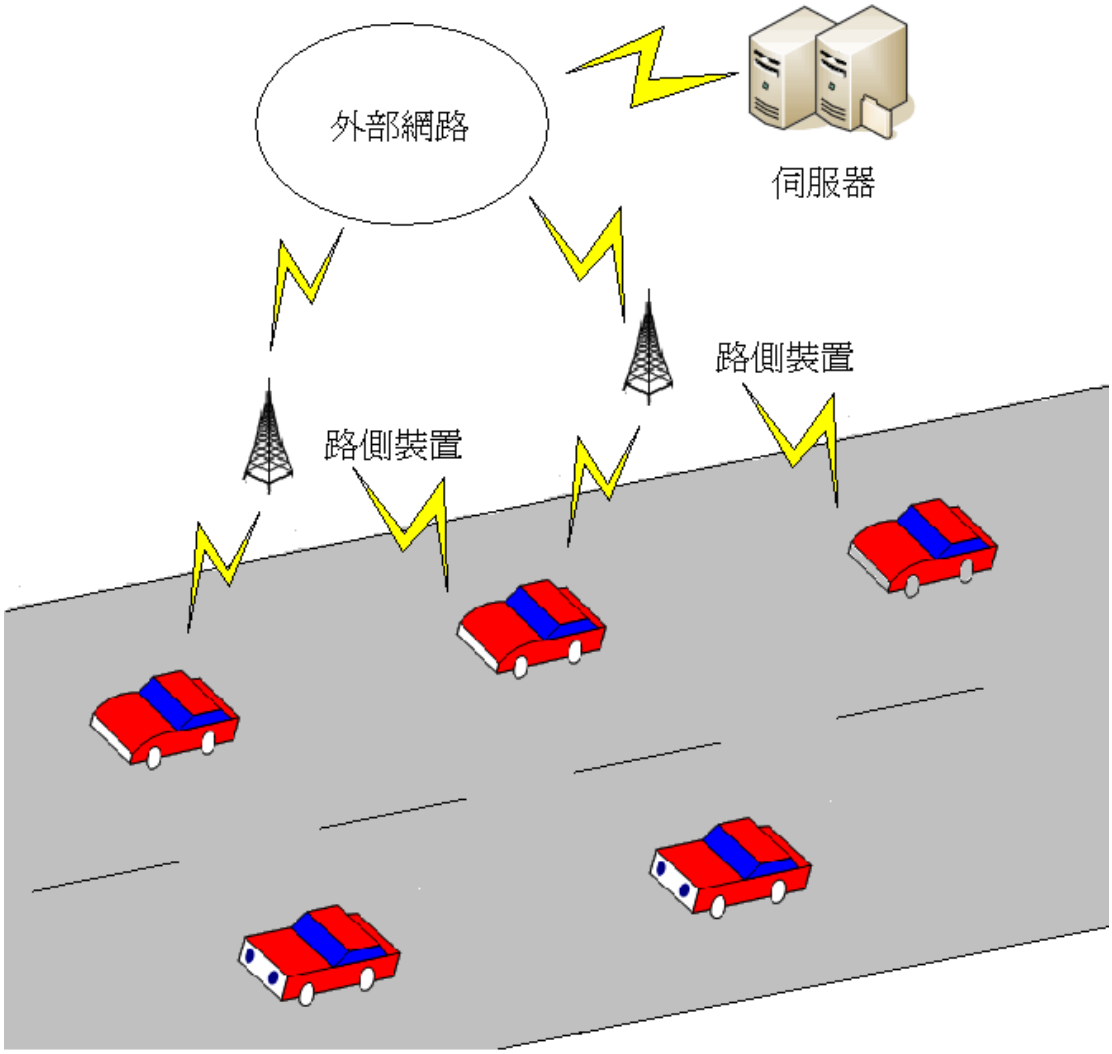


圖 2.1 車路通訊示意圖

- 車間通訊(Inter-Vehicle Communication, IVC) (Little & Agarwal, 2005)

如圖 2.2 所示，車輛會透過車上配置的車載機(On Board Unit, OBU)和其它車輛進行資訊的傳遞，不需要椅靠任何的 RSU。由於車輛之間沒有透過 RSU 去維持彼此之間位置的關係，因此在傳輸的過程中，便可能因為離開可傳輸的範圍而造成封包傳輸失敗。再者，如果接收者和傳輸者不在彼此的傳輸範圍內，則傳送必須透過多點跳躍(Multi - hop)的方式傳送，但這種傳輸方式也可能因為途中的轉送節點離開傳輸範圍或離開道路，造成封包的傳送失敗。

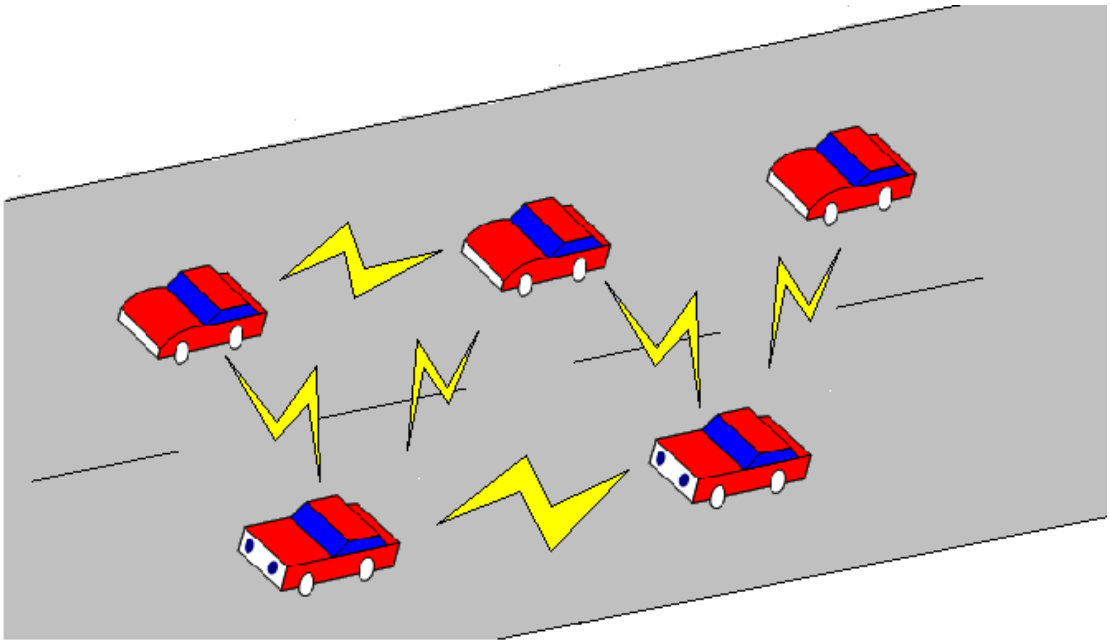


圖 2.2 車間通訊示意圖

- 結合 RVC 和 IVC 的網路架構 (Taleb, Ochi, Jamalipour, Nei, & Nemoto, 2006; Yanlin, Abichar, & Chang, 2006)

結合 RVC 和 IVC 的架構，可以當車輛和車輛因為距離過遠無法傳送封包的時候，透過 RSU 快速的傳遞資訊，此時 RSU 同時扮演著閘道器和傳遞資訊的轉送節點，如圖 2.3 所示。因為 RSU 之間是用有線網路連接，所以在傳送的速度、效率上都比透過多點跳躍的方式傳送資訊要好。

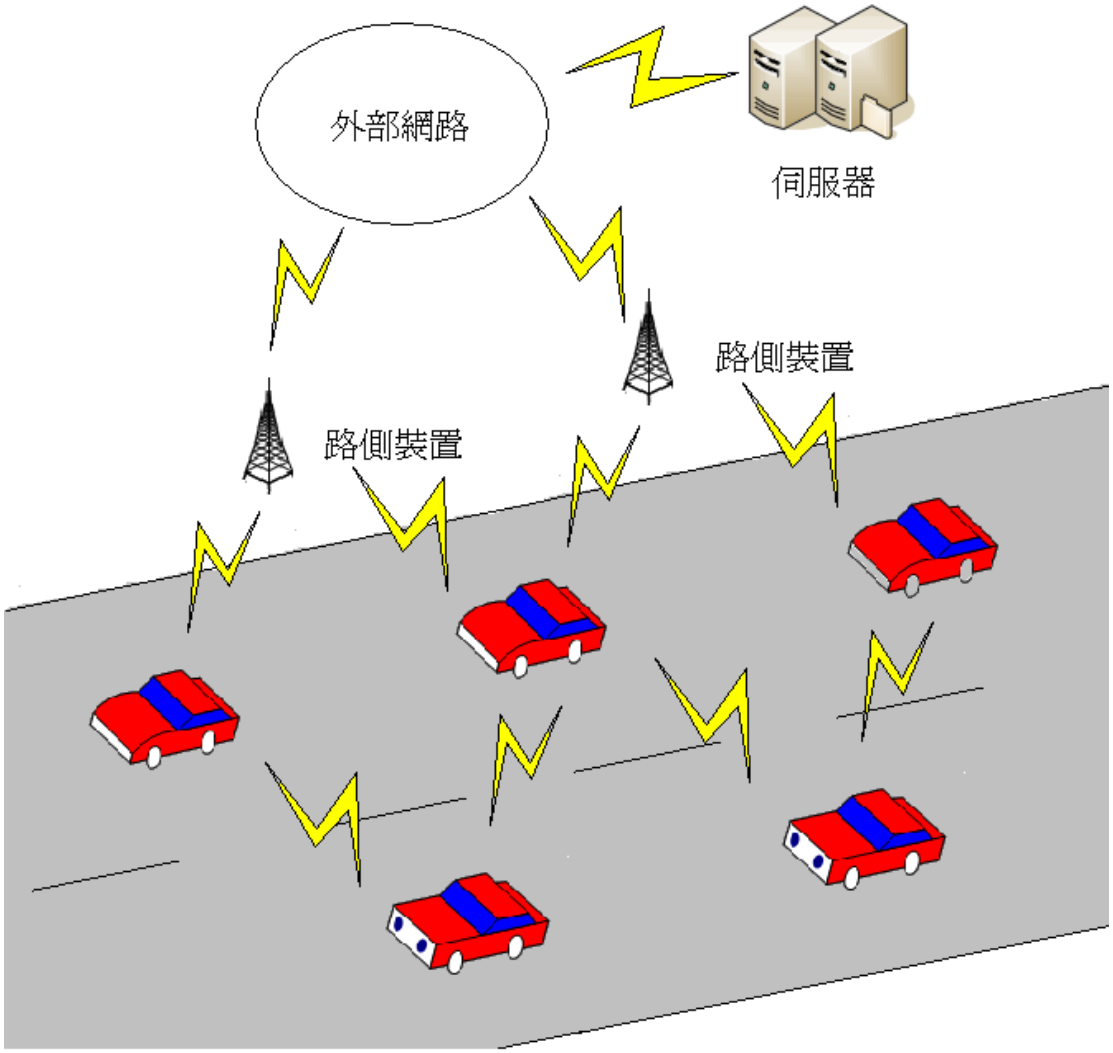


圖 2.3 結合 RVC 與 IVC 的網路架構示意圖

2.1.4 VANET 之應用

VANET 的應用非常廣泛，可概分為安全性和便利性兩大類。在安全性的應用上，包括緊急事件與安全訊息的傳遞，例如前方發生碰撞事故、緊急煞車、橋樑斷裂等等緊急事件，需要將情況傳送給事故地點鄰近的車輛，以便事先做好接下來的行駛規劃或其它因應的措施，避免造成更大的事故發生。這種緊急的訊息，在傳送的時候應給予最高的優先權來處理。

在便利性的應用上，大致可分為三類：

1. 多媒體娛樂應用：駕駛人和乘客可以在車中享受多媒體影音服務，不論是收聽音樂、影片、檔案的傳輸等等。車輛間亦可以形成公開或私人的群組來分享多媒體服務，例如一群人相約出去，在路上需要知道彼此的相關位置，便可以形成一個語音聯絡的群組，可隨時得知彼此的動態狀況。

2. 商業廣告發佈：駕駛人可以主動接收、查詢，或是採取訂閱的方式來獲得資訊。例如，駕駛人訂閱特定商家的購物資訊，或者經過某些店家的時候，會自動接收店家提供的最新購物資訊；或是告知店家附設停車場的停車位資訊，期望駕駛人進來消費。商家可以利用 VANET 提供各種加值服務。

3. 即時的交通路況更新：車輛透過 RSU，將行車資訊傳回區域的控管中心做資料的整合，控管中心再將整合過的資訊透過 RSU 來發送最新的交通路況報導。或是車輛間彼此傳送訊息，再利用 OBU 將最即時的路況資訊做整合。交通路況的更新有利於用車人可以提前規劃行車路線，以期達到最佳的行車路況。

Ohara, Nojima, & Ishibuchi (2007)提出了一個車間通訊路由(Inter-Vehicle Communication route)的路徑導航演算法，當對向的車輛彼此擦身而過時，會透過 IVC，彼此分享路況資訊。如圖 2.4 所示，A 車和 B 車彼此分享資訊，根據估計的時間權重值去更新每條道路的旅行時間，再根據新的路況資訊去做路徑導航，找出到目的地的最短時間路線。

A

道路編號	旅行時間	時間估計權重值
1	7	7
2	5	12
3	8	20
4	3	23

道路編號	旅行時間	時間估計權重值
1	5	25
2	6	20
3	8	20
4	3	23

B

道路編號	旅行時間	時間估計權重值
1	5	25
2	6	20
3	9	14
4	5	5

道路編號	旅行時間	時間估計權重值
1	5	25
2	6	20
3	8	20
4	3	23

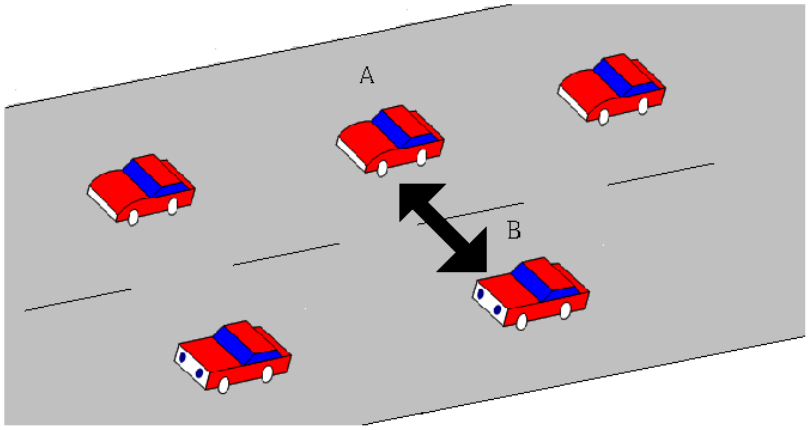


圖 2.4 車間通訊路由-路況資訊交換示意圖

2.1.5 VANET 的節點移動模式

在 VANET 環境中行進的車輛，在以往的研究中，其行駛環境不是高速公路就是網格式的路網。以高速公路而言，車輛的移動方式是固定的，因此車輛能做的可能是改變車輛速度，或是以機率的方式去決定車輛是否變換車道 (Toh, 2002)；對於網格式的路網，如圖 2.5 所示，有城市區段移動模式(City Section) (Bechler & Wolf, 2005)，隨機的產生目的地之後，用最短路徑朝目的地前進。至於真實路網的移動方式，則是利用亂數產生目的地後，再利用 Dijkstar 演算法求出車輛到目的地的最短路徑 (Marco, Jerome, Fethi, & Christian, 2007)，車輛再依照此最短路徑移動到目的地。

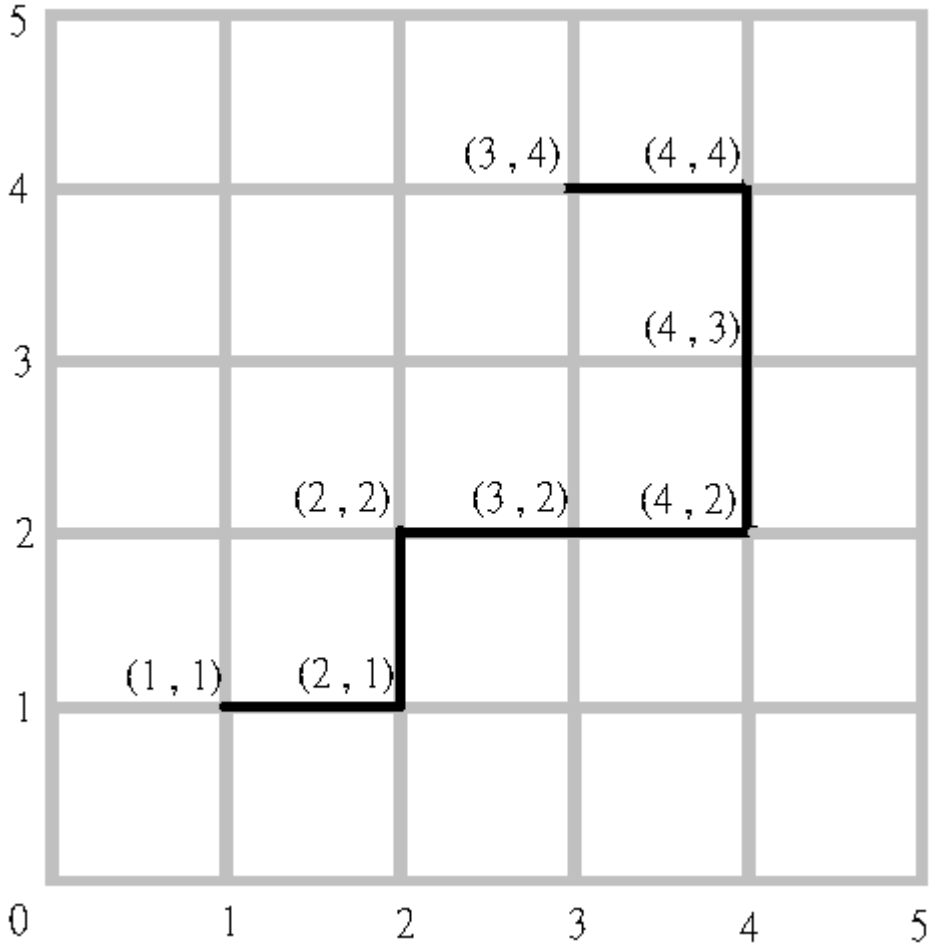


圖 2.5 城市區段移動模式

2.2 囚犯困境

1950 年，由就職於蘭德公司的弗勒德(M. Flood)和德雷希爾(M. Dresher)擬定出相關困境的理論，後來由顧問塔克(A. Tucker)以囚犯方式闡述，並命名為「囚犯困境」。囚犯困境是一個明確的數學模型，很頻繁的被經濟學者 (Kofman & Lawarree, 1996)、社會學家 (Surbey & McNally, 1997; Rabow, 1988)、政治學者 (Uno & Namatame, 1999)、生物學家 (Legge, 1996)、心理學家 (Boone, Brabander, & Witteloostuijn, 1999)用來分析利益的衝突。

典型的囚犯困境如下。警方抓到了甲、乙兩名嫌疑犯，但沒足夠的證據指控

兩人有罪。因此警方將兩人分開，分別和兩人見面，並向兩人提出下列三點相同的選擇：

- 若一人認罪並作證檢控對方，而對方保持沉默，此人將即時獲釋，沉默者將判監十年。
- 若二人都保持沉默，則二人同樣判監半年。
- 若二人都互相檢舉，則二人同樣判監兩年。

其中，囚犯困境假設每個囚犯都會尋求最大的自身利益，不關心另一個囚犯的利益。

囚犯應該選擇檢舉對方或是保持沉默，才能讓自己的刑期最短?由於兩人被分開囚禁，所以不知道對方會如何選擇，即使雙方可以交談，但是不能保證最後不會被對方背叛。所以就私人利益而言，檢舉對方會比保持沉默所獲得的刑期較低。由於兩人情況相同，所以兩人的結論都會是選擇背叛，結果兩人同樣判監兩年。可是以公共利益而言，如果兩人合作都保持沉默，只會被判刑半年，整體來說利益最高。但根據假設，兩人都是理性的個人，追求個人最大的利益，導致兩人選擇的都是背叛對方，結果兩人被判監的時間大於合作的時間要多。這就是「困境」所在。

將囚犯困境問題用一般形式表示。兩個參與者可以自己決定選擇合作或是背叛，接著根據兩個人的選擇，可以得到如表 2.1 的收益矩陣。

表 2.1 囚犯困境收益矩陣

甲 / 乙	合作	背叛
合作	合作 報酬	背叛誘惑 受騙支付
背叛	受騙支付 背叛誘惑	背叛 懲罰

其中四個結果的價值比較可用下列的不等式表示之

背叛誘惑>合作報酬>背叛懲罰>受騙支付

在本篇研究中，反社會行為的車輛的出現，可能的其中一個原因便是受到背叛所能得到的最佳利益誘惑，因而發送經過修改的訊息，使自己的行車路況更好。

2.3 在車間通訊中封包的廣播

在 VANET 的環境中，因為車輛是不停的以高速移動，所以網路拓樸一直呈現變動的狀態，因此資訊的散佈幾乎都使用廣播的方式。可是廣播的方式會使網路中的廣播封包過多，造成效能的降低，為此在許多的研究中，便考慮環境變因去減少網路中的廣播封包。在本節中的兩個小節會介紹兩種減少網路中廣播封包的傳遞機制。

2.3.1 貪婪轉送(Greedy Forwarding)

Karp & Kung (2000)提出貪婪轉送的方式傳送封包，節點會在傳輸範圍內找一個離目標節點最近的節點當作轉送點，依此類推直到封包傳送到目標節點，在這個方式下轉送點變少，廣播封包相對的也會減少。如圖 2.6 所示，每次都會確保挑選的是區域最佳的節點。

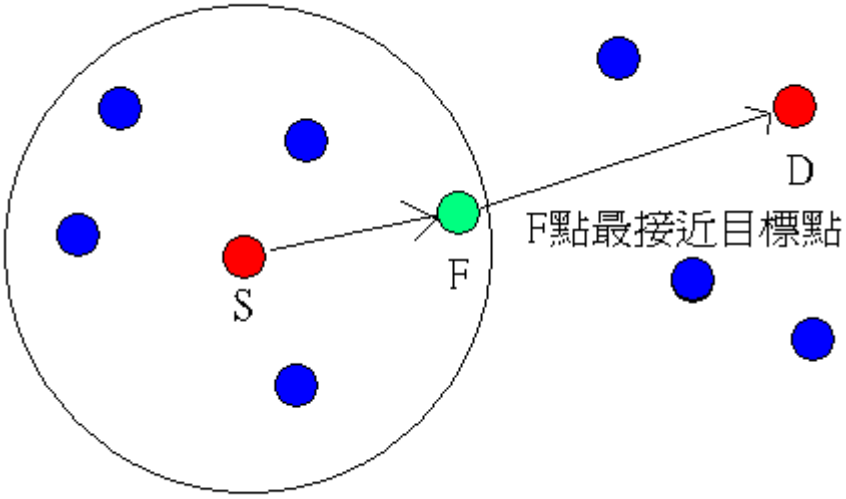


圖 2.6 貪婪轉送示意圖

可是貪婪轉送可能會遇到一個問題，就是當轉送點已經是距離目標節點最近的一個點，但目標節點不在傳輸範圍內，且兩點之間不存在其它節點，此時貪婪轉送便無法使用。如圖 2.7 所示，F 點被選為轉送點，但是 F 點和 D 點已經超出了傳輸距離，無法一次就傳送到，因此貪婪轉送的方法不能使用。為了解決這個問題， Karp 和 Kung 提出利用右手法則(Right-Hand Rule)的方法去解決這個問題，其方法是繞著中間空掉區域的節點做傳送，亦即封包的傳送路徑為

。

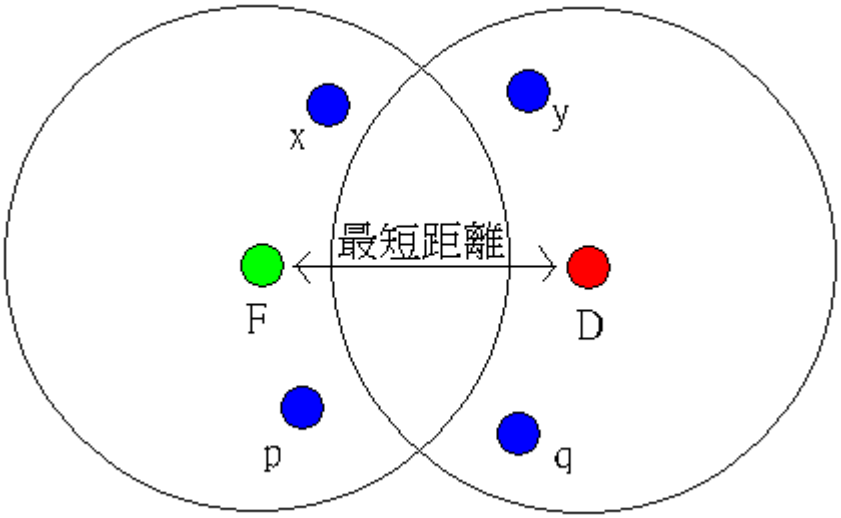


圖 2.7 貪婪轉送問題示意圖

2.3.2 散佈函數機制(Propagation Function)

Costa, Frey, Migliavacca, & Mottola (2006)提出散佈函數的概念，此函數可以將環境參數轉換成數值，藉由比較數值計算出適合傳遞封包的節點。如圖 2.8 所示，利用最簡單的距離公式來當作散佈函數計算出自身和目標節點的權重值。當節點收到封包的時候，會根據封包內的散佈函數計算本身的權重值，再利用封包內的發送者位置，計算出發送者的權重值，相比較就可以決定是否繼續傳送廣播封包。因此 X 點和 Y 點會繼續傳送廣播封包，而 Z 點因為和目標節 D 為反方向，故不傳送。和一般的廣播方式相較之下，變少了一個方向的封包數量。

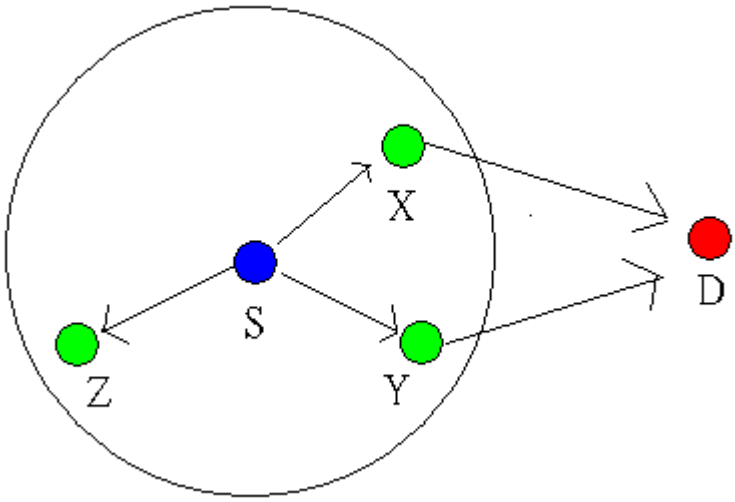


圖 2.8 散佈函數示意圖

為了讓封包進一步減少並且保有一定的散佈率，Costa, Frey, Migliavacca, & Mottola (2006)結合 Gossip-based ad hoc routing (Li, Rus, & Haas, 2002)，利用機率和距離的方式來決定是否繼續傳送封包。當車輛收到封包時，利用無線訊號可以得知雙方的距離，再將此距離拿來除以可傳輸範圍，可以得到一個比值，接著產生一個隨機亂數，用之前產生的比值作為臨界值，兩個數拿來比較，若亂數值小於臨界值則進行資訊的傳送。

在整個資訊傳送的過程中，訊息封包都是用廣播的形式發送，在收到封包後，再由收到封包的節點決定要不要繼續傳送封包，而不是發送者本身，所以這個機制屬於分散式的散佈機制，可以應用在廣大的區域。

可是在資訊傳送的過程中，當兩台車的距離太遠導致於法傳送資訊，會發生封包無法傳送出去的問題，如圖 2.9 所示，當廣播封包從發送者傳送過兩台車輛後，發現下一台車的位置超過了可傳輸範圍，導致封包無法進行傳送的動作。

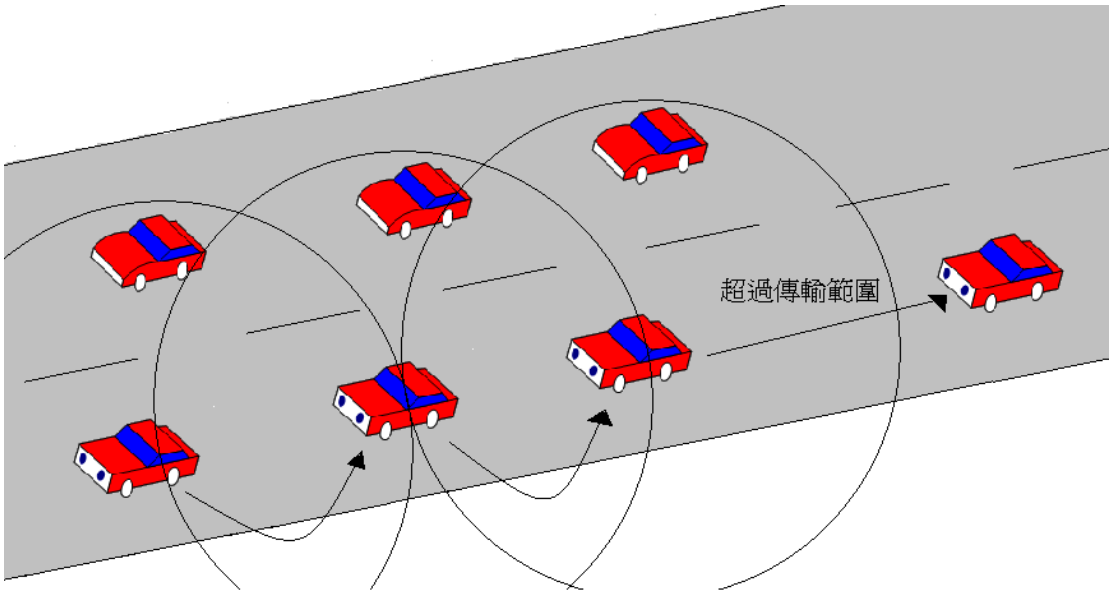


圖 2.9 車間通訊問題示意圖

針對這個問題，可以用 store and forward 的方式進行資訊的傳送。當資訊傳遞時，會為每筆資訊都設定一個重傳的計時器，在經過散佈函數計算過後，符合條件將會發送廣播封包，並將資訊放進自身的訊息佇列，並為訊息設定一個倒數計時器，當計時器時間到就重新發送封包。主要的原因是在發送廣播封包時，並不會收到對方的回應封包，所以不能確定對方是否接收到了封包訊息，只有當對方也發送相同的封包時，才能確定對方的存在。當收到相同的封包時，會查看訊息佇列中是否有相同的封包，並比較來源位置和自身位置離目標位置的遠近，如果來源位置離目標位置較近，則可以推測封包已經傳遞出去，這時便可以停止計時器；如果沒有收到封包資訊，表示沒有其它車輛將資訊傳送出去，這時便繼續進行重送的動作，直到將資訊封包傳送出去。

2.4 VANET 中的威脅模型

Lin, Sun, & Shen (2007)和 Yan, Olariu, & Weigle (2008)在個別的研究中，都有對 VANET 中的威脅模型做出整理，綜合整理可以細分為八種不同的類型：

1. 偽造訊息攻擊(Bogus information attack)：威脅者可能為了某些特定的目的傳送偽造訊息。例如，威脅車輛傳送一個偽造的交通阻塞訊息給前車，讓前車以為前方道路塞車，使得前車往其它方向行進，而自己可以得到一個好的交通路況。

2. 越權先佔攻擊(Unauthorized preemption attack)：在很多地方的路旁基礎建設，如紅綠燈，可以為了某些特殊情況提供特別的交通優先權。可能是學區的紅綠燈，在上下學的時候為了兒童的安全而被控制；或是為了讓救護車、警車和消防車有較好的路況而被控制。類似一次偽造訊息攻擊，威脅者可能為了得到一個更好的交通路況，而非法的控制紅綠燈。

3. 訊息重送攻擊(Message replay attack)：威脅者可能為了擾亂交通，在某些特定的時刻重送正確的封包。

4. 訊息修改攻擊(Message modification attack)：訊息可能在傳送之前或之後被修改。威脅者透過自身的設備在傳送之前改變訊息的來源或內容，例如：威脅者肇事逃逸，為了躲避警方的追查，進而修改自身的位置或時間訊息；或是威脅者修改了前方車禍所發出的緊急訊息，降低其它駕駛者的戒心。

5. 偽裝身份攻擊(Impersonation attack)：威脅者可能偽裝成另一輛車，以圖欺騙其它車輛或是路側裝置。

6. 路旁基礎建設複製攻擊(RSU replication attack)：由於目前存在大量的路旁基礎建設，為了要妥善保護這些基礎建設免受惡意的攻擊需要不少的費用，也因此在經費有限的情況下，可能導致某些基礎建設被威脅者給侵佔。之後，威脅者可能利用奪取的基礎建設發動所有惡意的攻擊，例

如：廣播偽造的交通訊息。

7. 阻斷服務攻擊(Denial-of-service attack)：威脅者傳送毫不相關的大量訊息去佔用頻寬還有消耗其它車輛的計算資源 (Liu & Yu, 2006)。

8. 移動追蹤(Movement tracking)：因為無線通訊是一個共有且公開的媒介，所以威脅者可以很容易的進行竊聽。威脅者可能在某一個地區攔截到巨大數量的訊息，便可以通過訊息分析，根據車輛的物理位置和移動的情況去追蹤車輛。

在 IVC 中的威脅模型有偽造訊息攻擊、訊息重送攻擊、訊息修改攻擊、偽裝身份攻擊和阻斷服務攻擊五種。其中，可以在封包格式中使用時戳（timestamp）避免訊息重送攻擊（Yan, Olariu, & Weigle, 2008）；訊息修改攻擊可以透過收集其它車道的訊息封包來達到破解的作用；偽裝身份攻擊則可以在車輛上加入地圖歷史（map history)來破解。在車間通訊的阻斷服務攻擊，當威脅車輛攻擊其它車輛時，也會讓自己造成頻寬過載的現象，故阻斷服務攻擊多著重在攻擊車路通訊中的路側裝置或伺服器等等，可以使用網路監控程式偵測部分的阻斷服務攻擊。

其它知名的攻擊還有 Sybil 攻擊，威脅者偽造多個身分並且發送出去，這些錯誤的身分會使路上的其它車輛造成幻覺，也因此會對 VANET 造成嚴重的影響。例如：碰撞警告系統可能因為偽造的車輛位置，以為即將發生事故，提醒司機應該迅速煞車，而造成一次真正的事故發生。

Leinmuller, Schoch, Kargl, & Maihofer (2005)提出了一個威脅模型，威脅者透過偽造自身位置資訊，可以進一步的攔截道路上所有的訊息。如圖 2.10 所示，當 B 車要將訊息從左邊傳送到右邊時，因為車輛在傳送訊息時，會將訊息傳送

給距離目的地最近的車輛當作轉送者，因此一開始 B 車會依照規則將訊息傳送給 C 車，可是當 C 車要發送訊息時，A 車透過修改自身位置為 Ar 這個位置，使得 C 車以為 A 車的位置比較靠近目的地，因而將資訊傳送給 A 車，依此類推，左邊要發送到右邊的訊息都會被 A 車給攔截。同理，右邊要發送到左邊的訊息也會被 A 車用同樣的方法給攔截。因此，只要透過修改自身位置資訊，便可以攔截整個道路上的訊息封包，而且威脅者可以肆意的修改這些訊息或是將這些訊息給刪除，使得道路安全受到憂慮。在此威脅模型中，封包成功傳送率下降 50%。

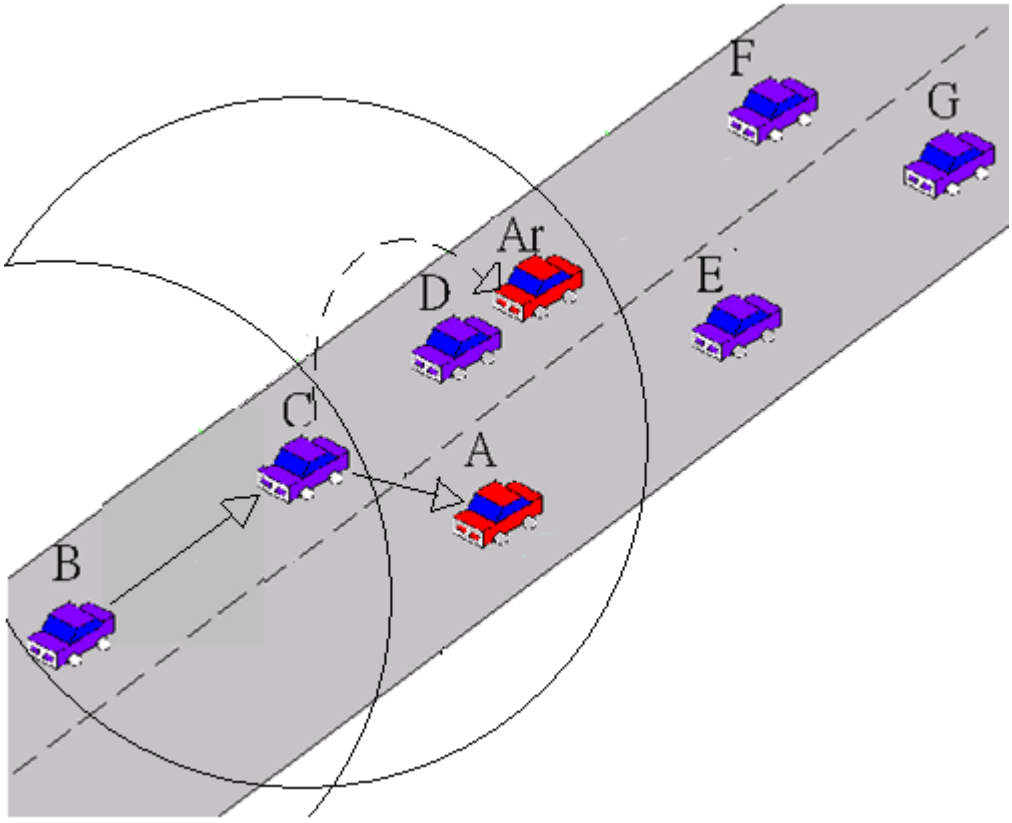


圖 2.10 錯誤位置訊息攻擊

隔年，Leinmuller, Schoch, & Kargl (2006)使用竊聽的驗證方法去進行模擬。如圖 2.11 所示，假設每台車可以在自身的傳輸範圍內，去竊聽其它車輛傳送封包的情況，可是在兩種情況下，可以偵測到威脅者的存在：

1. 當 D 車將訊息傳送給 A 車後，此時 A 車透過距離機制，會將訊息傳送

給 E 車。D 車透過竊聽，會發現自身擁有的訊息是 A 車的位置比 E 車位置更靠近目的地，但 A 車卻將訊息傳送給 E 車，由此可知 A 車是威脅者。

2. 當 C 車要發送訊息，透過距離機制應該發送訊息給 E 車，可是 A 車偽造位置資訊而使 C 車傳送訊息給它。D 車透過竊聽，得知 C 車傳送訊息給 A 車，可是卻發現自身擁有的資訊，A 車會在 C 車的可傳輸範圍外，由此可發現 A 車是威脅者。

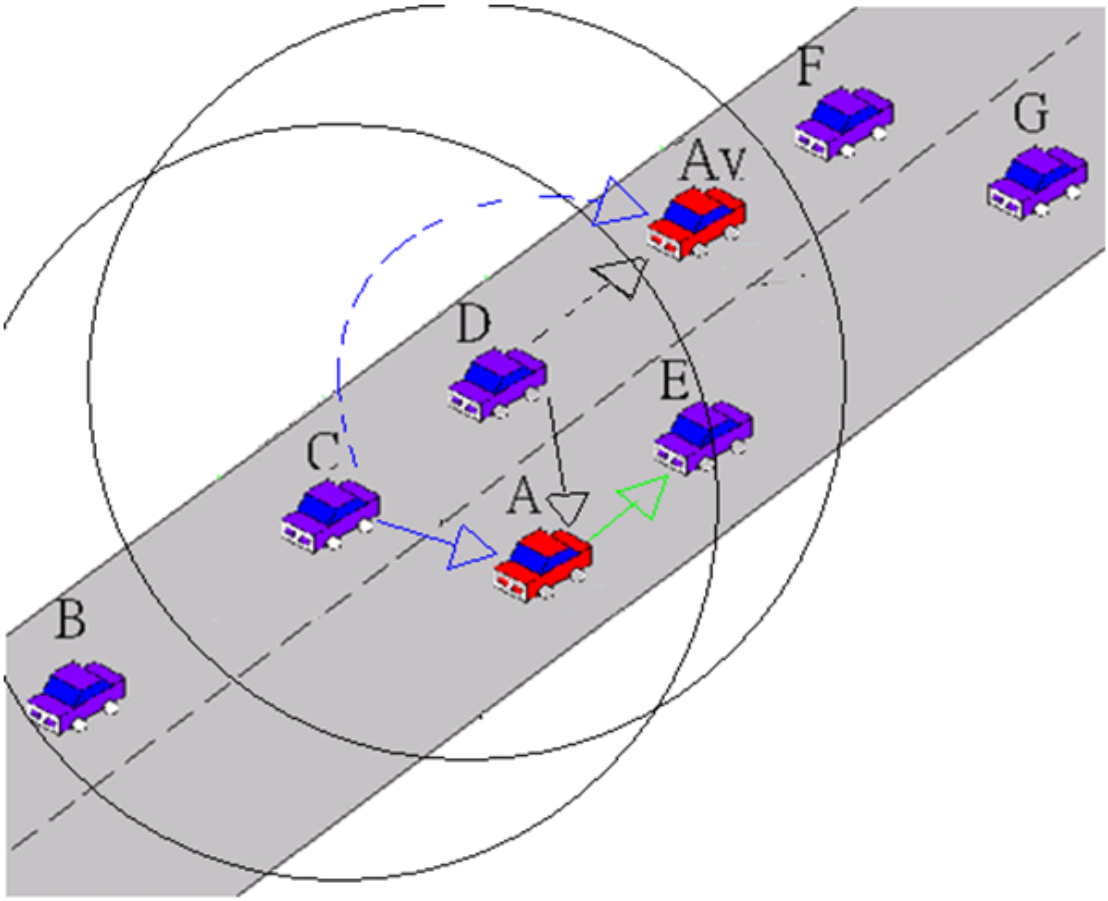


圖 2.11 驗證方法(竊聽)

使用竊聽的方法進行驗證，在最佳的情況下，封包成功傳送率可以高達 95%。

Yan, Olariu, & Weigle (2008)在研究中提出，在某些情況下，還是難以偵測到威脅者的存在。如圖 2.12 所示，A 車是威脅者，且前後各被兩台車輛平行的阻

攔，五輛車分開維持相對的距離，大約是一個可傳輸範圍的半徑。因為 A 車在四台車的中心，可能是這個區域的封包轉送者，可以收到其它車輛的封包訊息，如果 A 車任意的修改封包內容，卻因為這四輛車的阻攔，使得雷達無法使用，造成驗證上是很困難的。這種情況從微觀來看，可能會造成影響；可是從宏觀的角度來看，當這種車輛數量不多的時候，其實是可以被忽略掉的。

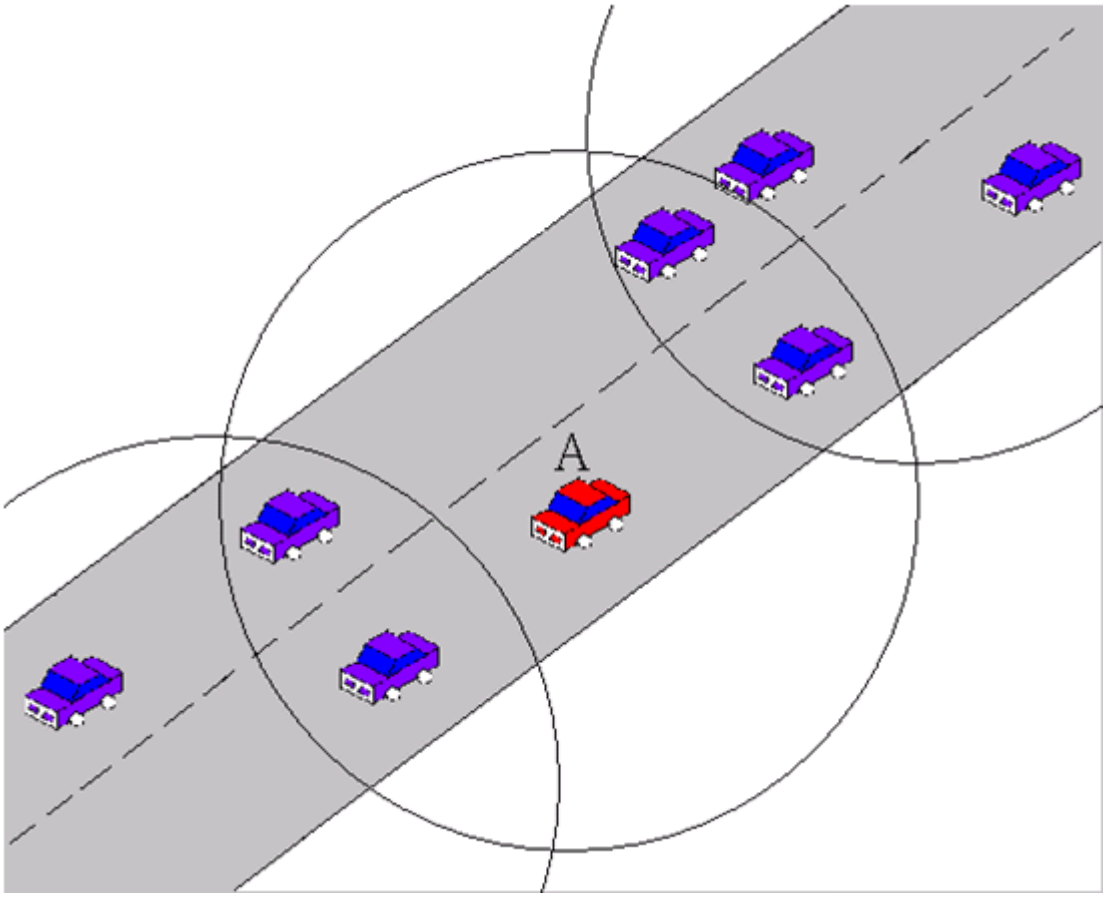


圖 2.12 威脅車輛難以被偵測的情況

威脅車輛經過查獲也會遭到懲罰。根據是否有做上線認證的動作，可以將處罰的方式分為兩種。車輛只要上路則會跟控管中心做認證的動作，此種車輛只要被查獲使用威脅攻擊，則會撤銷其會員的身份，之後某些服務則不能再使用；車輛上路不用做認證動作的環境，車輛使用了威脅攻擊被查獲後，則控管中心會將此車輛的 ID 加入黑名單，透過 RVC 將黑名單傳達給路上的車輛知道，車輛透過黑名單可以有效排除這些車輛傳送的訊息封包。

綜合以上，威脅車輛雖然可以透過攻擊別人取得自己想要獲得的利益，但是也必須冒著風險承擔被查獲後的處罰。雖然可以透過更換 OBU 來繼續使用服務，但金錢的損耗則是再次可以正常使用 VANET 服務的處罰。

第三章 研究方法

在本章中，描述了本研究所使用的研究方法。第一節針對整體系統進行詳細的描述，第二節詳細的描述實驗設計，包括會使用到的各種路況更新方法和不同的威脅車輛種類，以及各種參數的設定，第三節說明進行效能評估時所使用到的評估指標，第四節則說明了與真實路網密度是如何對照。

3.1 系統描述

本研究使用 C 語言直接開發模擬系統。在模擬系統中，建構了網狀的路網、建立了基本的車輛移動模型，也模擬了網路封包的傳遞，車輛間透過封包的傳送，分享彼此的路況資訊，車輛透過車載機將路況資訊做整合，再根據新的路況資訊使用 Dijkstra 演算法做出路徑規劃，並且立刻改變其移動模式，往目的地前進。在本節中，第一小節會介紹網狀路網的模型，第二小節會說明整體的系統架構，第三小節會詳談系統的流程，第四小節會說明車輛移動模式，第五小節會說明網路層面中訊息封包的傳送方法。

3.1.1 模擬模型

如圖 3.1 所示，本研究用細胞自動機模型為基本模型，建構出模擬時車輛所使用的底層路網模型。由於本研究著重在威脅車輛的種類和各種路況更新方法之間的效能，所以簡化了路網的複雜度。對路網的基本假設如下：

1、 道路為單線雙向道：我們假設每條道路都是單線雙向道，亦即每個車行方向都只有一個線道，所以每臺車輛都會受同線道的前方車輛影響而改變自身的

車速，也不會有超車的狀況發生。

2、 街道長度為 50 個網格大小：對每個街道的長度都設為 50。

3、 車輛皆為小客車：為了便於計算一個網格的大小以及降低複雜度，所以車輛的種類只考慮小客車，每臺車輛會佔用一個網格的大小。

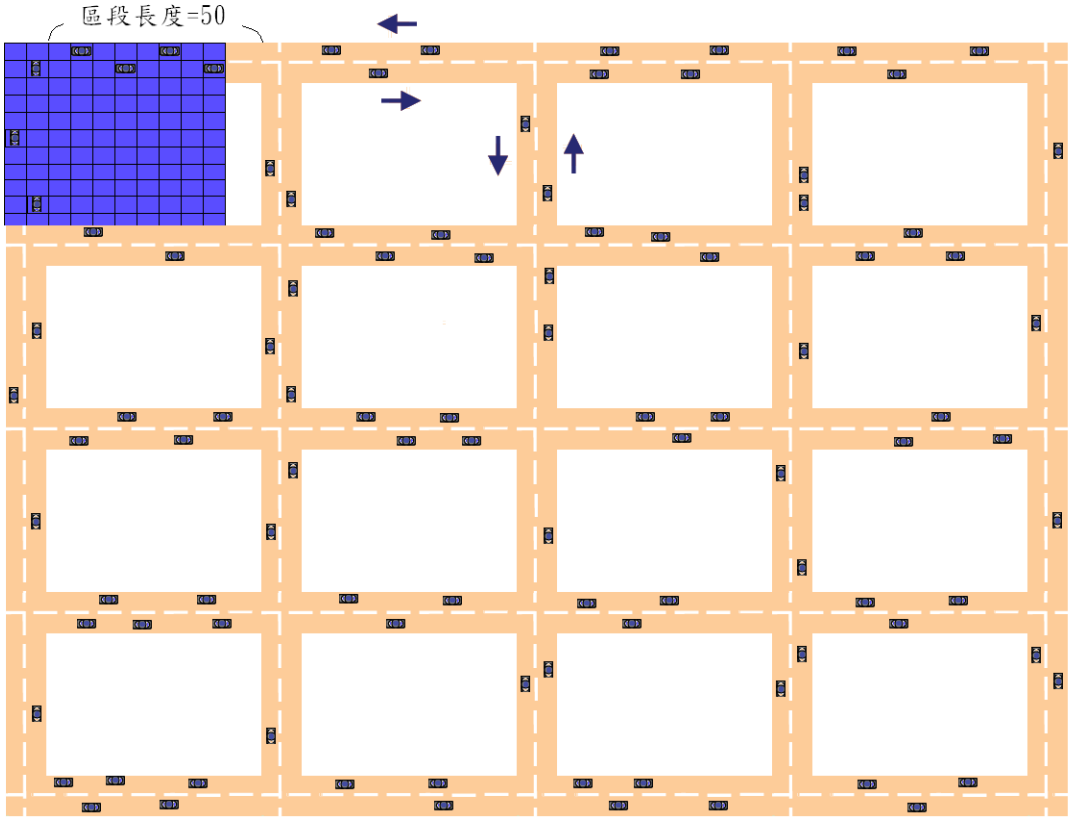


圖 3.1 路網示意圖

在本研究中所使用的路網模型，是五條縱向車道和五條橫向車道交錯而成的網格式路網，所以路網中共會有 40 條街道和 25 個路口。其中每條街道都是長度為 50 個網格大小的單線雙向道，所以在街道的部分共有 4000 個網格；每個路口都是由 4 個網格所組成，所以在街口的部分共有 100 個網格。計算街道和路口的網格數目，可以計算出本研究中車輛所能行駛的網格數為 4100 個。

3.1.2 系統架構

如圖 3.1 所示，Global 代表的是整個模擬環境，其中包含了三個主要的副程式，Topology、Network 和 RoadModel。每一個副程式的說明如下：

1、 RoadModel：主要是用來建立整個路網環境。在模擬時，會先初始路網的資訊，當車輛進行初始位置設置還有開始移動時，將會使用到此路網資料，以確保車輛確實在道路上行駛。

2、 Topology：主要是用來建立車輛間底層的網路拓樸資料。會根據車輛訊息的可傳輸範圍大小，建立車輛和車輛之間的拓樸關係。每當車輛進行移動，位置有所變更後，因為有些車輛會離開車輛的可傳輸範圍，也有些車輛會進入此車輛的可傳輸範圍，因此其網路拓樸也必須重新建立。

3、 Network：主要用來傳送網路封包。在模擬時，會維持一個訊息佇列，用來儲存所需被發送的封包資訊，接著會利用到 Topology 中的網路拓樸資訊，來找出可傳輸範圍內的所有車輛，來進行網路的廣播封包傳送。

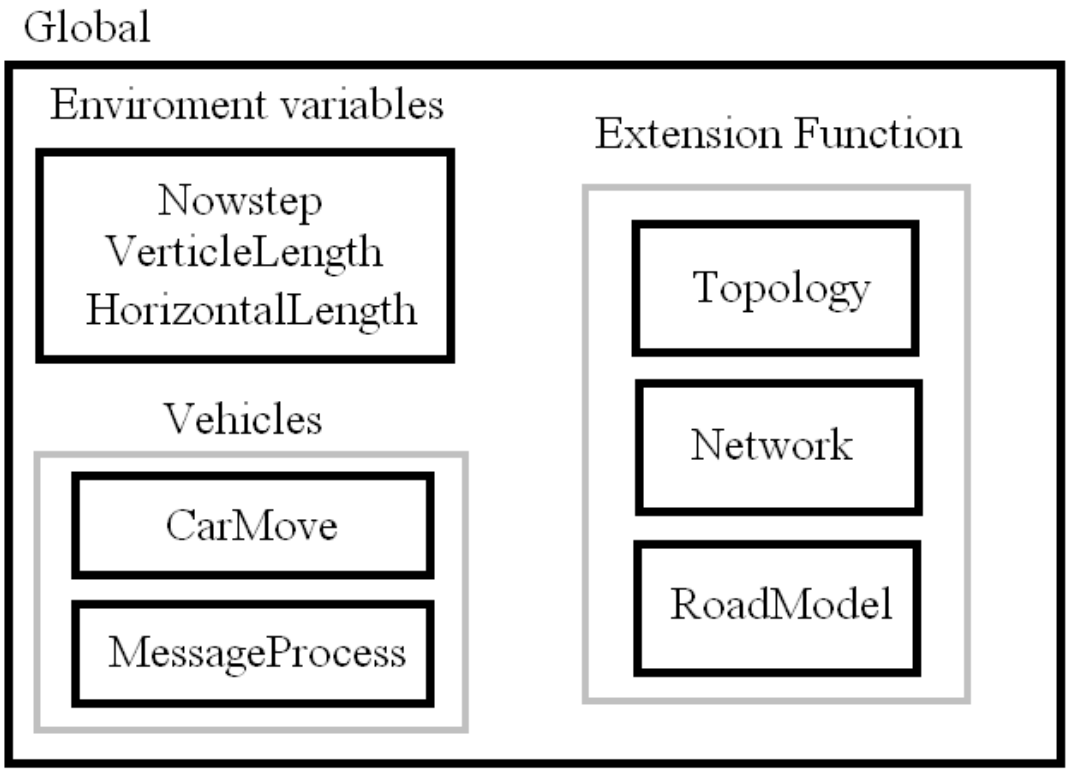


圖 3.2 系統架構

在本研究的模擬系統中，事件的執行方式是循環執行的，因此在 Global 中的環境參數需要用 Nowstep 紀錄模擬目前的時間，而 VerticleLength 和 HorizontalLength 則會分別紀錄網狀路網的大小，這兩個參數在設置初始變數時會被設定，在建構 RoadModel 時會被使用。在系統中，車輛的模擬是另外獨立出來的，其中，每台車輛都會有路況資訊的處理機制(MessageProcess)和車輛移動的機制(CarMove)。

3.1.3 系統流程

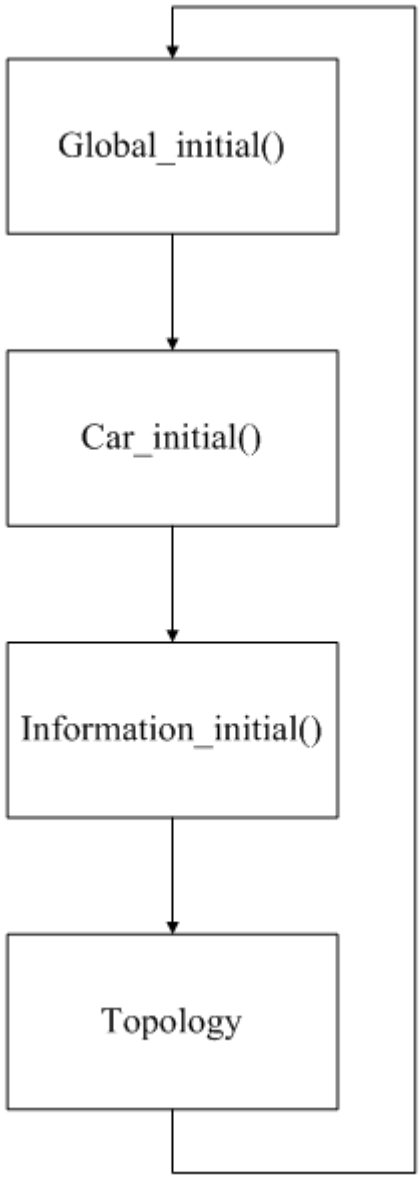


圖 3.3 系統初始化流程

圖 3.3 說明系統初始化的流程。模擬一開始會讀取設定檔，讀取完後會呼叫 Global_initial()進行環境變數的設定以及進行初始化，主要是設定車輛的初始位置還有產生目的地位置，因為車輛是在道路上行駛，所以會根據路網的資訊來隨機選取兩個位置給每台車輛，分別作為現在位置和目的地位置。在車輛位置初始

化完畢後，在進行網路拓樸的建立，主要是為了維護車輛之間的鄰居關係，當需要進行訊息廣播時，便可以利用這個拓樸資訊得知可以接收到訊息的車輛。

圖 3.4 呈現的是整個系統的流程，在模擬系統中是採取循環執行的方式。一開始車輛會從網路拓樸中，去接收鄰居車輛發送出來的廣播封包，其中會包含每臺車輛對於自身所擁有的路況資訊，亦即每條街道的旅行時間和時戳(街道旅行時間更新後存活的時間)。接著車輛會根據接收到的路況資訊去更新自身的路況資訊，在這裡路況資訊更新會有最新時戳法則、加權時戳法則、地理+最新時戳法則、地理+加權時戳法則四種不同的方法，關於路況資訊更新方法細節的部分我們會在後面的小節中討論。由於車輛會有每條街區的旅行時間，所以在路徑導航的部分，我們將每個路口視為一個點，街道的旅行時間看作連接此街道的一個路口到下一個路口的值(亦即兩點之間有線相接)，因此可以透過使用 Dijkstra 演算法，找出到達目的地時間最短的最佳路徑。然後車輛會按照規劃的路徑進行移動，我們會在下一小節討論車輛的移動。車輛移動之後，會根據車輛最新的位置來更新網路拓樸，找出每台車的鄰居車輛是哪些。最後再處理車輛的行為，亦即根據網路拓樸，將自身所保存的路況資訊發送給鄰居車輛。

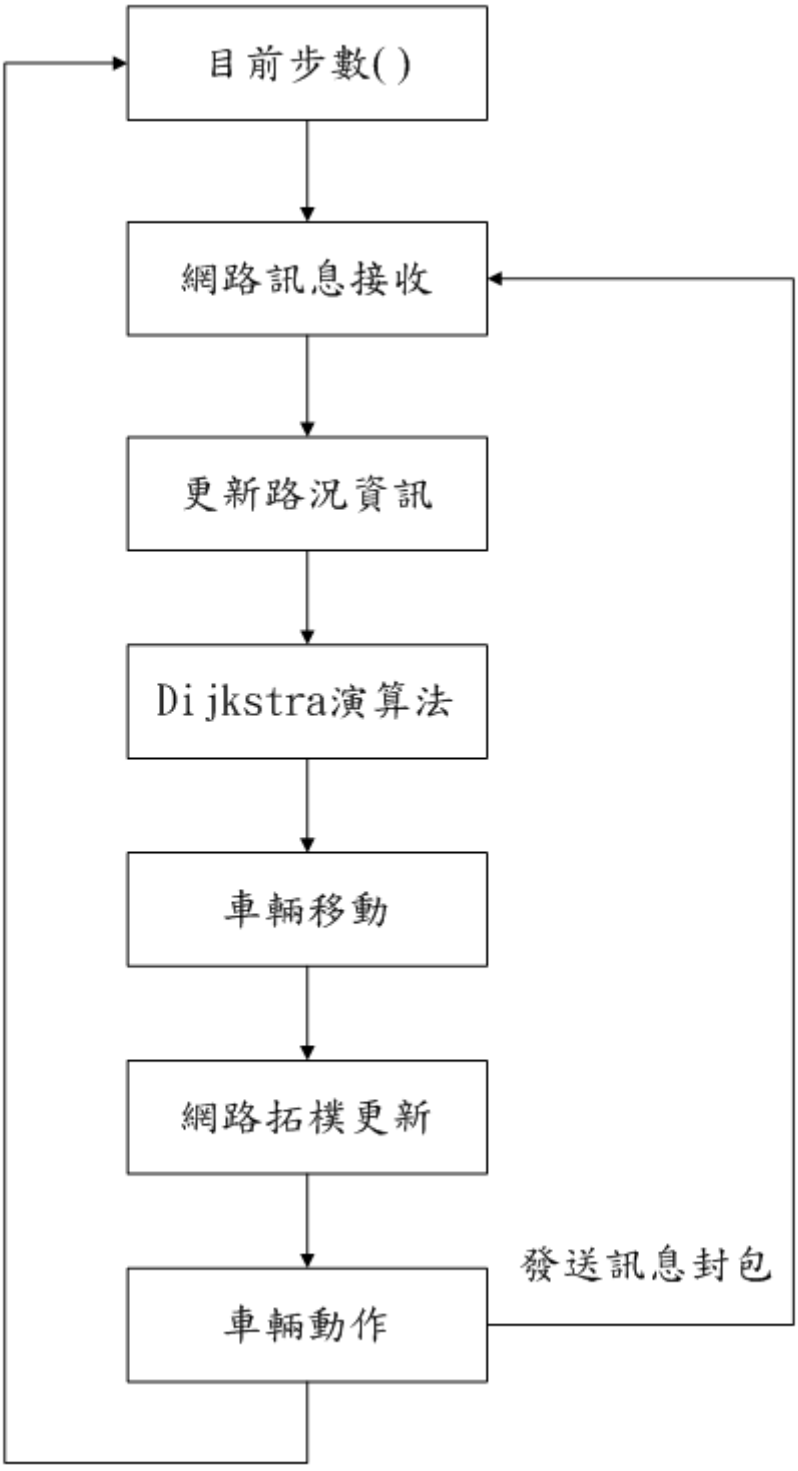


圖 3.4 訊息流程圖

3.1.4 車輛移動模式

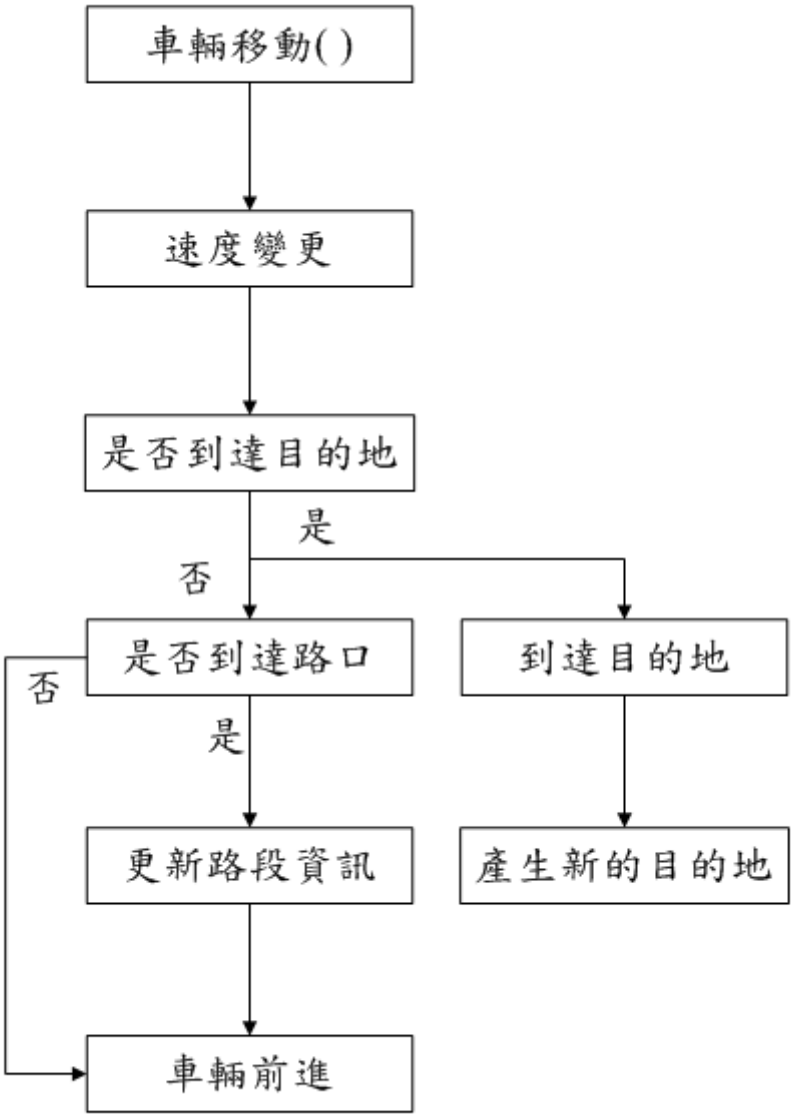


圖 3.5 車輛移動流程圖

如圖 3.5 所示，表示的是車輛移動的流程圖。當系統跑完 Dijkstra 演算法後，會呼叫車輛移動( )此函數開始進行車輛的移動。一開始車輛會透過速度的改變，確保車輛在移動時，不會與同向車道前方的車輛相碰撞。接著再偵測是否到達目的地或是路口，如果到達目的地，就移動到目的地，同時目的地變成新的起點並

且產生一個新的目的地，讓車輛可以繼續保持行進的狀態；如果車輛行駛到路口時，則會根據剛行駛完的路段的旅行時間，將自身關於此路段的旅行時間更新，並給更新的路段資訊一個存活時間，以便在車輛進行路況資訊更新時，可以去存取作為比較的變數。

在產生新的目的地這邊，Marco, Jerome, Fethi, & Christian (2007)在其研究中，用亂數產生一個目的地，再利用 Dijkstar 演算法找出車輛到目的地的最短路徑，接著車輛按照其產生的路徑進行移動。一般而言，亂數產生一個目的地，產生的目的地可以平均的分散於路網中，可是和真實世界相比較，某些特定的地點會有許多人前往，如購物商城、公司、學校等等。因此，在本實驗中，一開始會亂數選取路網中的某些點，讓其被選到的機率比其它位置高，所以當車輛在路網中移動時，在這些點周圍的車流密度會較高。就宏觀來看，整個路網也比較符合真實世界的路況。

在車輛速度的變化，採取固定的速度或是隨機產生一個速度進行模擬，這樣速度的變化都過於單調，對此部分，我們採用一個車輛速度變化的演算法，符合真實車輛速度變化的規則又不複雜。對於車輛，會給予最大與最小速度以及加速度 1，在車輛初始配置時，會給予車輛速度為零，接下來利用設定的加速度來改變車輛的速度。車速會按照下列兩個步驟做車速的更新：

(1) 加速：車速 V < MaxV，且與前車距離小於(V+1)，則車速提升到 V+1。

(2) 減速：在位置 i 的車輛看見前車在位置 i+j，且 j < V，車速降為 j-1。

3.1.5 訊息封包傳送

在本研究，封包的傳送方式都是使用廣播的形式進行，亦即以發送者為中

心，在可傳輸範圍內的所有車輛，都可以接收到發送者發送的訊息封包。

在系統中，當車輛接收到資訊後，便會進行路況資訊的更新，之後車輛發送的訊息都會是更新過後的路況資訊。在我們的研究中，封包的傳送是利用單點跳躍(Single - hop)的形式在網路拓樸中傳遞，亦即廣播封包只會傳送一次，而接收者並不會再將封包傳送出去。

3.2 實驗設計

在本研究的底層模型是路徑導航的模型，我們加入威脅車輛，並且透過修改路網密度和威脅車輛的比例作為參數的調整，去比較在不同的威脅車輛種類中，各種不同的路況更新方法，哪種路況更新方法的效能會較佳。在本節中，第一小節會說明不同的路況更新方法，第二小節會說明不同的威脅車輛種類，第三小節則是介紹實驗中會進行的參數調整。

3.2.1 路況資訊更新的方法

在本研究中，當車輛收到廣播封包後，我們會使用不同的路況資訊更新方法。透過使用不同的更新方法，討論在哪種情況下正常車輛會有較佳的效能。除了使用最新時戳法則和加權時戳法則這兩種基本的路況更新方法；為了探討地理位置對路況更新的影響，還使用了考慮地理相對位置這個要素，分別搭配最新時戳法則和加權時戳法則這兩種更新方法。在實驗中用了下列四種不同的更新方法：

(1) 最新時戳法則

此種方式主要是比較資訊產生的時間，亦即當車輛行駛過某條路段後，會將

行駛這條路段的旅行時間設定為此路段的權重，此時設定一個會隨時間增加的參數來標記此路段更新之後的存活時間，我們將此參數命名為時戳。時戳愈小，表示此路段的旅行時間存活時間短，亦即此路段資訊很新；時戳愈大，表示此路段的旅行時間存活時間愈長，亦即此路段資訊很舊了。如圖 3.6 所示，當 A 車收到了 B 車發送出來的路況資訊封包，便開始比較每條路段的時戳，時戳時間小的，A 車會將其相對應的權重值更新為此路段的權重，依此類推，直到 A 車整個路網的路段資訊都做過更新。

A

道路編號	旅行時間	時戳
1	7	7
2	5	12
3	8	20
4	3	23

B

道路編號	旅行時間	時戳
1	5	25
2	6	20
3	9	14
4	5	5

A

道路編號	旅行時間	時戳
1	7	7
2	5	12
3	9	14
4	5	5

圖 3.6 最新時戳法則範例

(2) 加權時戳法則

此種方式只要是依據時戳的大小，去求出一個比例權重給 n 筆資料的路段權重值，相乘後加總即為更新後的路段權重值。在這邊，時戳數字越小的，表示路段資訊愈新，所以會得到較大的比例權重，反之，時戳數字大的比例權重會越小，亦即比例權重和時戳數字大小會成反比。n 筆資料中第 m 筆資料的 A 路段比例權重為：

$$\frac{\frac{1}{T_{mA}}}{\sum_{i=1}^{n}\frac{1}{T_{iA}}}$$

其中，T_{iA}指的是第 i 筆資料中 A 路段的時戳值。

求出路段的比例權重後，將 n 筆資料的比例權重乘上路段權重後相加，便可以求得更新過後的路段權重值。同理，新的時戳值也用同樣的方式求得。式子如下列所示：

$$\text{新的 A 路段權重值} = W_{mA} \times \frac{\frac{1}{T_{mA}}}{\sum_{i=1}^{n}\frac{1}{T_{iA}}}$$

$$\text{新的 A 路段時戳值} = n \times \frac{\frac{1}{T_{mA}}}{\sum_{i=1}^{n}\frac{1}{T_{iA}}}$$

其中，W_{mA}指的是第 m 筆資料中 A 路段的權重值。

(3)、地理相對位置優先原則

此方法主要是依據發送者和接收者的相對方位，去決定路況更新的狀況。如圖 3.7，A 車收到了來自各個方位的路況資訊，其中，B 車在 A 車的右方，C 車在 A 車的上方，依照地理位置優先的概念，A 車在更新右方路段的資訊時，只會參考此時相對位置在 A 車右方的車輛，亦即會參考 B 車的資訊，而不參考 C 車的資訊。換言之，當 A 車更新上方路段的資訊時，只會參考 C 車和其它相對位置在 A 車上方的其它車輛。因為 B 車在 A 車的右方，當 B 車做路況更新的時候，便將右方的路況資訊更新過一次，而且在 B 車可傳輸範圍內的車輛，大部

分車輛都有右方路段的最新路況資訊，因此當 A 車更新右方路段的資訊時，B 車和 A 車右方車輛的路況資訊會比其它方位車輛的路況資訊來的準確、即時。

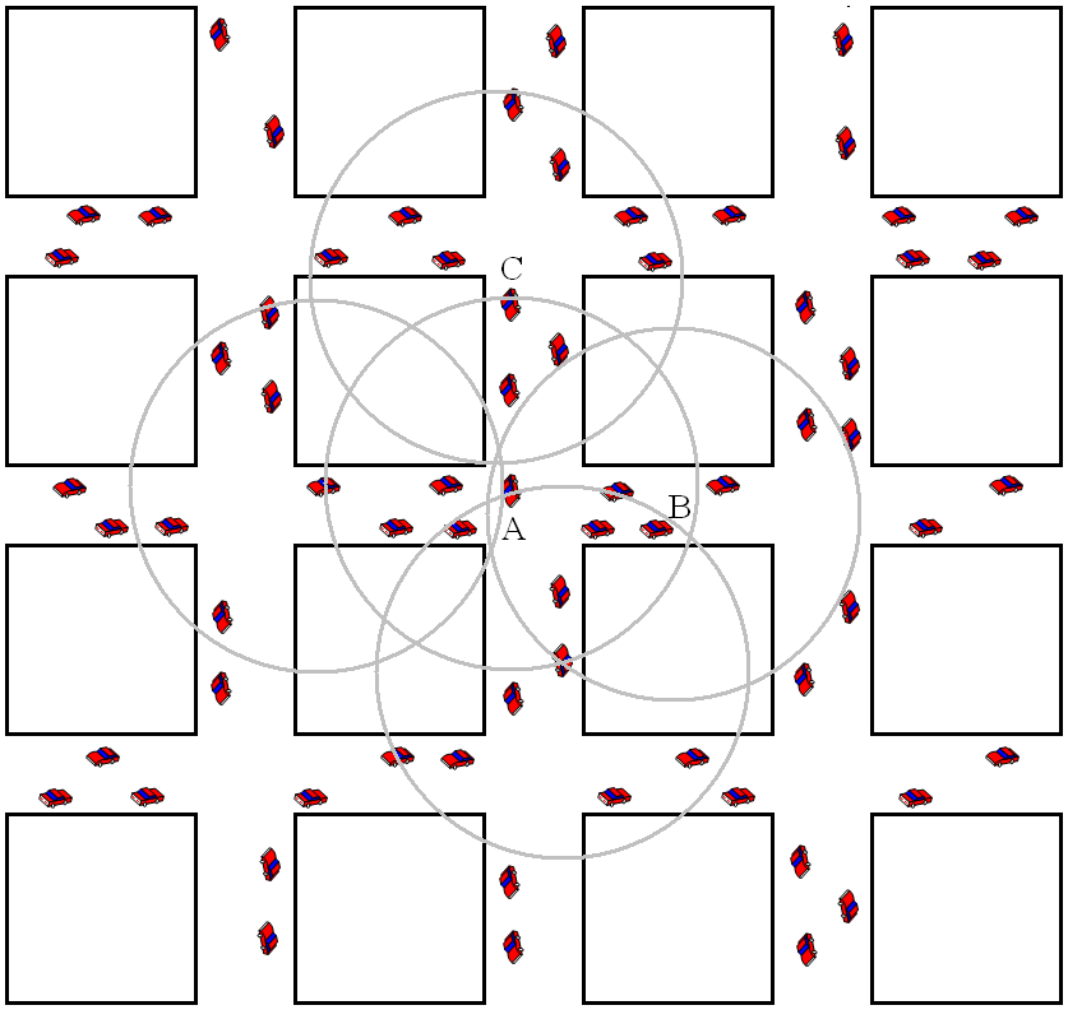


圖 3.7 考慮地理相對位置示意圖

關於地理位置方位的區分，如圖 3.8，是以進行路況更新的車輛為原點，將路網分成上、右、下、左四個相對的方位。然後在不同方位下的路況資訊更新方法，將會分別使用最新時戳法則和加權時戳法則為更新法則，透過混合的方式，希望能找出在各種狀況下效能的路況資訊更新方式。

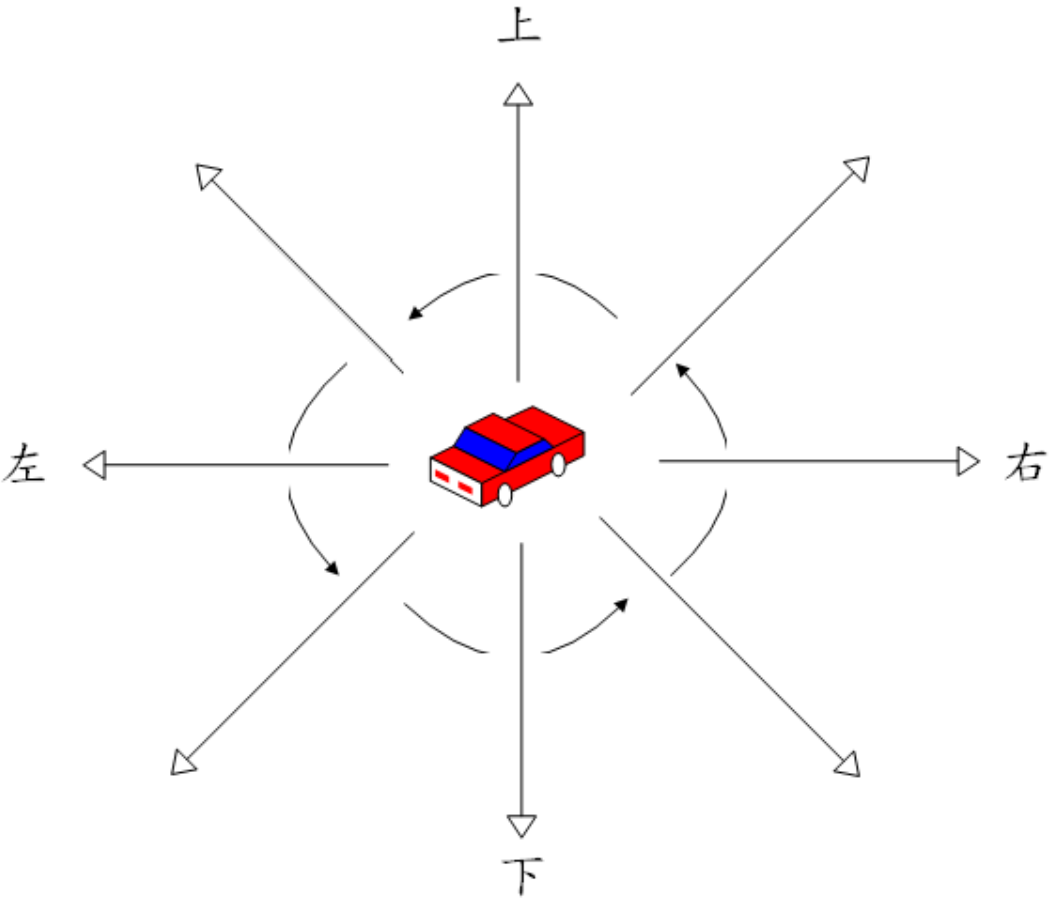


圖 3.8 方位區分示意圖

3.2.2 威脅車輛的種類

在實驗中的威脅車輛，為了讓自己經過路徑導航得到的路線，能夠保持道路暢通，因而透過修改路況資訊，將規劃好的路線會經過的所有路段權重值都增加，接著將錯誤的路況資訊發送出去，以圖其它車輛能夠繞開這些路段，讓自己有很好的行車路況。

我們會使用三種不同的威脅車輛種類來進行模擬。為了讓其它車輛繞開自己規劃好的路線，透過修改權重值來達成；為了讓其他車輛更能接受自己的路況資訊，透過修改時戳來達成。以上所述分別是偽造路況和偽造路況和時戳這兩種基本的威脅車輛種類。當威脅車輛將惡意封包訊息傳送出去，因為其它車輛更新路

況時接受惡意封包的訊息，因此也成為有惡意訊息的資訊。威脅車輛收到來自其它車輛的惡意封包訊息時，自身也會受到影響，因此我們提出了會考慮惡意封包訊息回向的第三種威脅車輛種類。在本研究中的三種威脅車輛種類如下：

(1) 偽造路況

如圖 3.9 所示，黑色實線是經過路徑導航規畫出來的最短時間路線，威脅車輛為了讓其它車輛繞開這些路段，所以會將最短時間路線上的所有路段權重值乘上三倍；黑色虛線是和最短時間路線相連的其它路段，為了讓其它車輛更有效的遠離，所以會將黑色虛線的所有路段權重值乘上二倍；其它所有未修改過的路段皆為灰色線，為了儘量讓其他車輛行駛這些路線，因此會將灰色線的路段權重值乘上二分之一。

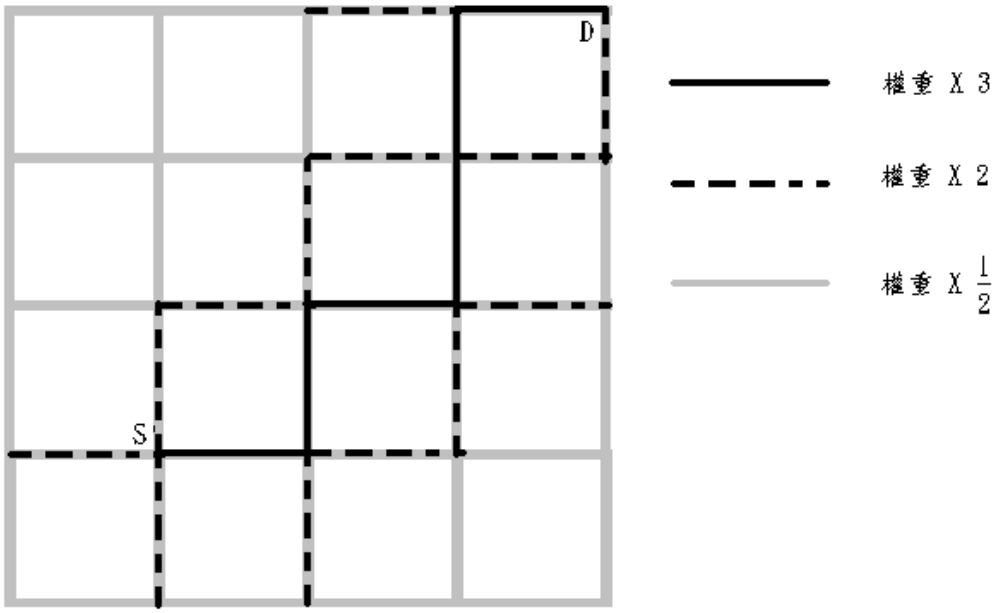


圖 3.9 修改權重示意圖

(2) 偽造路況和時戳

基於偽造路況的威脅車輛種類，這邊我們加上了時戳的修改。為了讓其它車

輛更容易接受威脅車輛修改過的路況資訊，透過修改時戳值來達成。最新時戳法則的路況更新方法會將路段資訊更新為最小的時戳值的路段資訊；加權時戳法則的路況更新方法則是用比例權重的方式來進行更新，亦即時戳值愈小，權重愈大，反之則權重值愈小。由上述，威脅車輛修改時戳值時，將時戳值修改成更小的值愈容易被接受。在修改權重、時戳的威脅車輛種類中，會將全部路段的時戳值乘上二分之一。

(3) 考慮惡意封包訊息回向

根據偽造路況和時戳的威脅車輛種類，我們加上了威脅車輛會考慮惡意封包訊息回向。由於威脅車輛將惡意封包訊息發送出去，因此在短時間內，從附近車輛收到的封包中，會有自己發送出去的惡意封包訊息。因此考慮惡意封包訊息回向的問題後，威脅車輛會在比對時戳值時，將其它車輛的時戳值乘上二倍，如果此時還是要進行路段資訊的更新，就不對其它車輛的路段權重值有任何的修改。

在上述的三種威脅車輛種類，有些都有乘上分數的情況，如遇上除不盡的狀況，便使用天花板函數取一個整數值。

3.2.3 參數的調整

在實驗中，為了模擬各種路網密度大小以及威脅車輛佔整體車輛的比例，我們會做的參數調整有以下兩種：

(1) 威脅車輛的比例：我們會去修改每次實驗中威脅車輛所佔的比例。有首項為5%、末項為50%、公差為5%的等差數列$\langle 5\%, 10\%, \ldots, 50\% \rangle$；有首項為1%、末項為32%、公比為2的等比數列$\langle 1\%, 2\%, \ldots, 32\% \rangle$。所以在實驗中會依照

數列$\langle 1\%, 2\%, 4\%, 5\%, 8\%, \ldots, 45\%, 50\% \rangle$依序去調整威脅車輛的比例，主要是幫助我們觀察，在不同的威脅車輛密度和路況更新方式下，威脅車輛所佔的比例，會發生怎樣的變化，例如：當威脅車輛變多，路網中的資訊紊亂，可能造成威脅車輛自己本身的效能也降低。

(2) 路網密度：我們直接透過改變整體車輛數目去模擬路網密度的變更。我們定義路網密度的公式如下：

$$\text{路網密度} = \frac{\text{總車輛數} \times \text{車輛面積}}{\text{路網道路面積}} = \frac{\text{總車輛數}}{\frac{\text{路網道路面積}}{\text{車輛面積}}}$$

其中，因為一臺車輛佔用一個網格大小，所以可以視為路網中車輛可以行駛的 4100 個網格數。在實驗中，會從 200 台車輛開始跑，每次增加 200 台，直到 1600 台車輛皆被模擬完畢；對照成路網密度，則是首項為 5%、末項為 40%、公差為 5%的等差數列$\langle 5\%, 10\%, \ldots, 40\% \rangle$。路網密度的大小，也會間接決定了錯誤資訊散佈的量的多寡。當密度大，每台車相對的可傳輸的車輛會變多，也因此錯誤資訊發送出去的量也變多，對路網造成的影響相對的變高。

3.3 效能指標

在本研究中，是在一個動態路徑導航系統下對威脅車輛進行容忍度分析，所以車輛從起始點到目的地的旅行時間(Travel_time)、旅行距離(Travel_distance)和最短距離(Shortest_distance)，都是重要的比較資訊。

Ohara, Nojima, & Ishibuchi (2007)提出Ⅱ和Ⅱ這兩個效能評估指標。Ⅱ是說一個

駕駛人從出發點距離它的目的地有多麼的接近，例如：如果II值愈小，表示該車輛距離目的地愈遠；II是在說明一個駕駛人從起點到達目的地的時間有多寬裕，如果II的值越小，表示駕駛者很舒適的接近它的目的地，亦即途中沒有遇到壅塞的路況。因為II只能表示車輛從起點到目的地有多遠，沒有辦法直接比較優劣；II表示了車輛行駛時是否擁塞，值愈小愈好，反之則愈差。所以在本研究中，採用擁塞I這個效能指標，這個效能指標被定義如下：

$$\text{擁塞度} = \frac{\text{旅行時間}}{\text{旅行距離}}$$

在本研究中，我們還採用另外一個效能指標：繞路比例。這個效能指標被定義如下：

$$\text{繞路比例} = \frac{\text{旅行距離} - \text{最短距離}}{\text{最短距離}}$$

在這邊我們想要觀察多跑的距離是最短距離的幾倍，藉由得到的比例去觀察不同的路況更新方法在不同的威脅車輛下的效能。在這邊，繞路比例值愈小，表示效能愈好，反之則愈差。

在本研究中，我們使用繞路比例和擁塞度這兩個效能指標，去評估不同路況資訊更新方法在各種狀況下的效能。最後會針對各種路網密度，透過效能的評估給出最佳的路況資訊更新方法。

3.4 路網密度

在本研究中，會根據路網的密度大小和各縣市的真實路網密度做出對應。路網密度的公式如下：

$$\text{路網密度} = \frac{\text{總車輛數} \times \text{停車格面積}}{\text{路網道路面積}} = \frac{\text{停車格面積}}{\frac{\text{路網道路面積}}{\text{總車輛數}}}$$

其中，停車格面積即為車輛面積。因為小客車並沒有特別規定長度，因此我們使用小客車的停車格面積來計算車輛面積。 表示的是每臺車輛享有的道路面積。

從道路交通標誌標線號誌設置規則第 190 條規定(交通部，98/12/08 修正)可以得知小型車停車位的尺寸。如表 3.1 所示，我們取長和寬的平均值來求停車格面積，亦即長度取 5.5 公尺，寬度取 2.25 公尺，則停車格面積取長與寬的乘積 12.375 平方公尺。

表 3.1 小型車尺寸設置規則

車種別	劃設線型及設置原則	尺寸
小型車 停車位	白實線，線寬10公分	長5～6公尺 寬2～2.5公尺

從行政院主計處可以找到各縣市的統計資訊，其中包含每汽車享有的道路面積。如表 3.2 所示，除了連江縣和金門縣，其它縣市皆可以找到相對應的數值。其中，車輛數是年底向各縣市監理機關領有統一牌照之汽車數量。

表 3.2 每汽車享有道路面積

	臺東縣	花蓮縣	嘉義市 高雄縣 嘉義縣	臺南縣 屏東縣	宜蘭縣 澎湖縣	雲林縣 南投縣	基隆市 苗栗縣	臺中縣	臺中市 臺南市 新竹縣	彰化縣	高雄市 新竹市 桃園縣	臺北市 臺北縣
每汽車享有道路面積 (平方公尺/輛)	150	130	120	110	100	90	80	70	60	50	40	30
路網密度	8%	9%	10%	11%	12%	13%	15%	17%	20%	24%	30%	40%

使用上述找到的停車格面積和每汽車享有道路面積，可以求出各縣市的路網密度。透過和真實路網密度的對照，可以讓本研究得到的結果更具實用性。

第四章 研究發現及分析

在本論文，我們提出了一個加入威脅車輛的路徑導航系統模型。在本章中，我們藉由調整參數對所提出的模型進行模擬和效能的評估，其中，我們會在三種不同的威脅車輛種類下，對路網的密度及威脅車輛的比例進行調整，以模擬不同的環境；而評估的項目有：網路惡意封包比例、車輛繞路比例和擁塞度。

在第一小節，我們將會介紹模擬環境的相關參數設定；在第二小節，對不同環境的模擬結果，探討網路惡意封包比例的變化；而第三小節，會針對車輛的繞路比例和擁塞度進行探討；最後在第四小節，會小結網路惡意封包比例和車輛的繞路比例和擁塞度分析得到的結果。

4.1 模擬環境設定

本論文的模擬環境以細胞自動機為基礎，建立了網格狀的交通道路模擬環境，並且配置了車輛和道路等物件，而其移動模式採用 2.1.4 小節中(Marco, Jerome, Fethi, & Christian (2007)所提出的城市區段移動模式。而本研究之參數設定如表 4.1。

表 4.1 模擬參數設定

模擬參數	數值
正常車輛通訊範圍	300m
威脅車輛通訊範圍	300m
觀察模擬次數	100 次
觀察模擬時間(回合數)	3000 回
路網車輛數目	200, 400, 600, 800, 1200, 1600(臺)
威脅車輛比例	1, 2, 4, 5, 8, 10, 15, 16, 20, 25, 30, 32, 35, 40, 45, 50(%)

本論文的觀察方式，是觀察在每次 3000 個回合數，模擬次數共 100 次所產

生之實驗數據結果取平均值後，並依據模擬實驗數據的平均值作出解釋。我們定義威脅車輛的車輛數目，是依據不同的路網車輛數目乘上威脅車輛比例所得到的定值，作為每回合威脅車輛的車輛總數，因此在一固定的路網車輛數目，根據不同的威脅車輛比例，會有十六種不同的威脅車輛數目。

而本論文的模擬，會在偽造路況、偽造路況和時戳以及考慮惡意封包訊息回向這三種威脅車輛種類下進行。根據不同的路網車輛數目和威脅車輛比例，在不同的環境下模擬三種威脅車輛種類。而模擬的結果分析，則會將模擬 3000 個回合數後的路網中所有的封包惡意程度加總並取其平均值，探討不同環境下的惡意封包變化情況；也會記錄車輛每次從起點到目的地的距離以及旅行時間和旅行距離，找出繞路比例和擁塞度的平均值去作效能的評估，探討三種威脅車輛種類和四種路況更新方法，會對車輛的效能有多大的影響，並根據不同環境找出最好的路況更新方法。

4.2 網路中惡意封包比例之分析

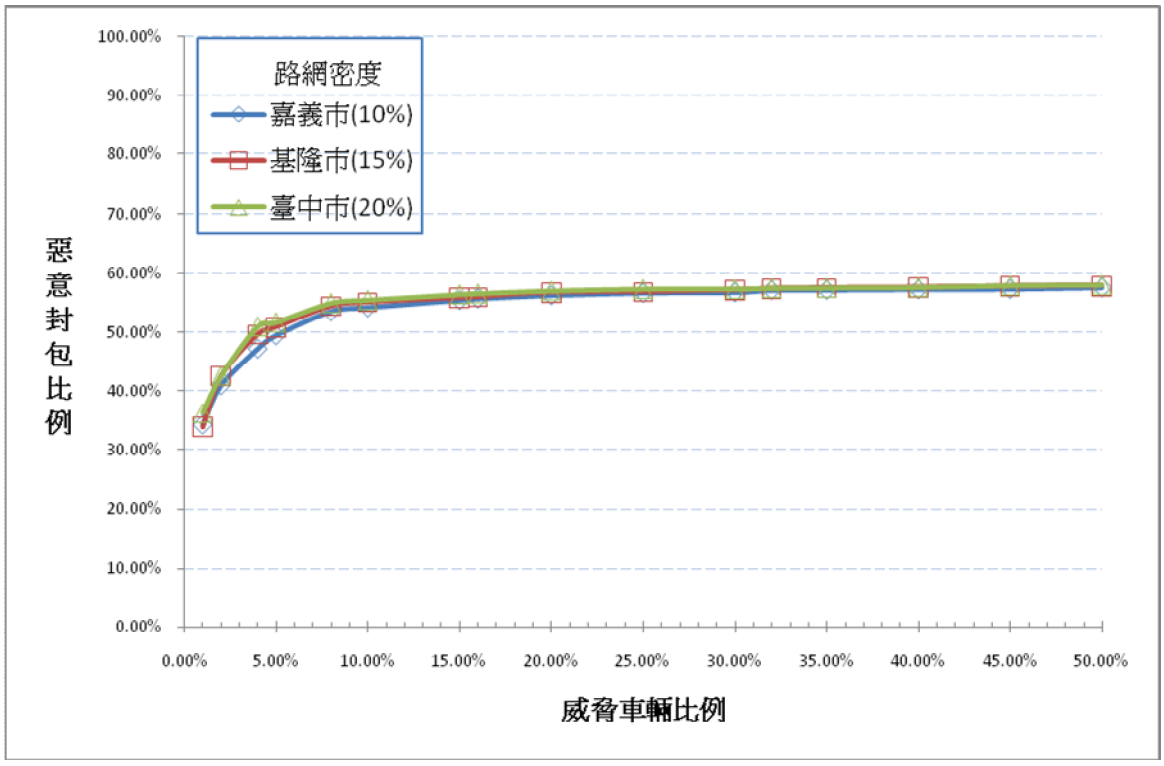
在本小節中，主要是在不同威脅車輛種類、不同路況更新方法以及不同的路網密度下，探討模擬到最後，網路中惡意封包占整體封包的比例之變化。首先，探討在不同路網密度下，不同路況更新方法和不同威脅車輛種類下，惡意封包訊息比例會呈現怎樣的變化；接著分析威脅車輛種類對路網的影響程度；最後再根據各種路況更新的方法，去探討網路中惡意封包訊息比例在不同路網密度和各種威脅車輛種類的變化。

4.2.1 路網密度對網路影響之分析

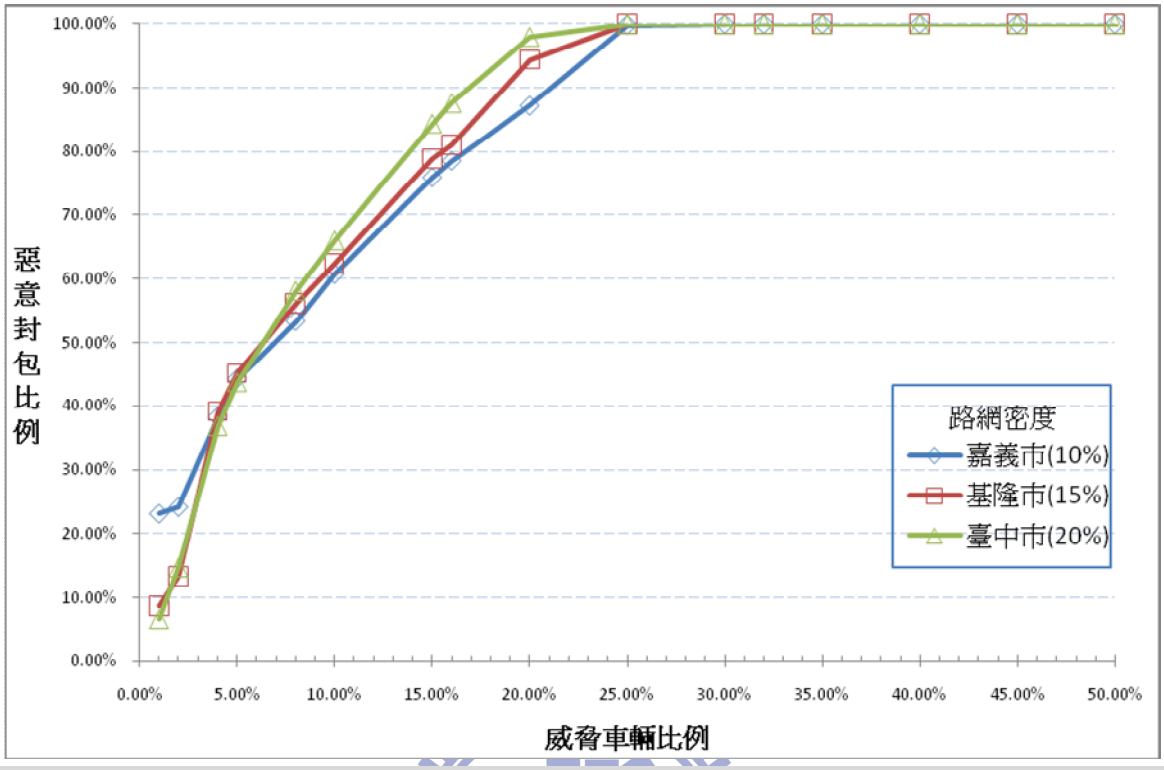
圖 4.1 主要是針對考慮惡意訊息回向的威脅車輛種類，在不同的路網密度、威脅車輛比例以及不同的路況更新方法進行的模擬。此圖的目的乃比較不同的路

網密度在不同的威脅車輛比例中，網路中的惡意封包訊息變化。可以發現最新時戳法則和地理+最新時戳法則路況更新方法，其惡意封包比例會依據路網密度的提高而略略的提高；加權時戳法則路況更新方法，在威脅車輛比例超過 5%，未達 25%以前，惡意封包比例會隨著路網密度的提高而提高，威脅車輛比例超過 25 之後，密度對其影響不大；而地理+加權時戳法則路況更新方法對密度的影響則沒有顯著的差別。由上，雖然有些模擬結果發現惡意封包比例會隨著路網密度變動，但差距不大，且模擬都會有誤差值，加上附錄 A 的另外兩種威脅車輛種類的模擬結果也呈現一樣的結果。推論路網密度對網路中的惡意封包比例在四種路況更新方法下皆沒有顯著的影響。

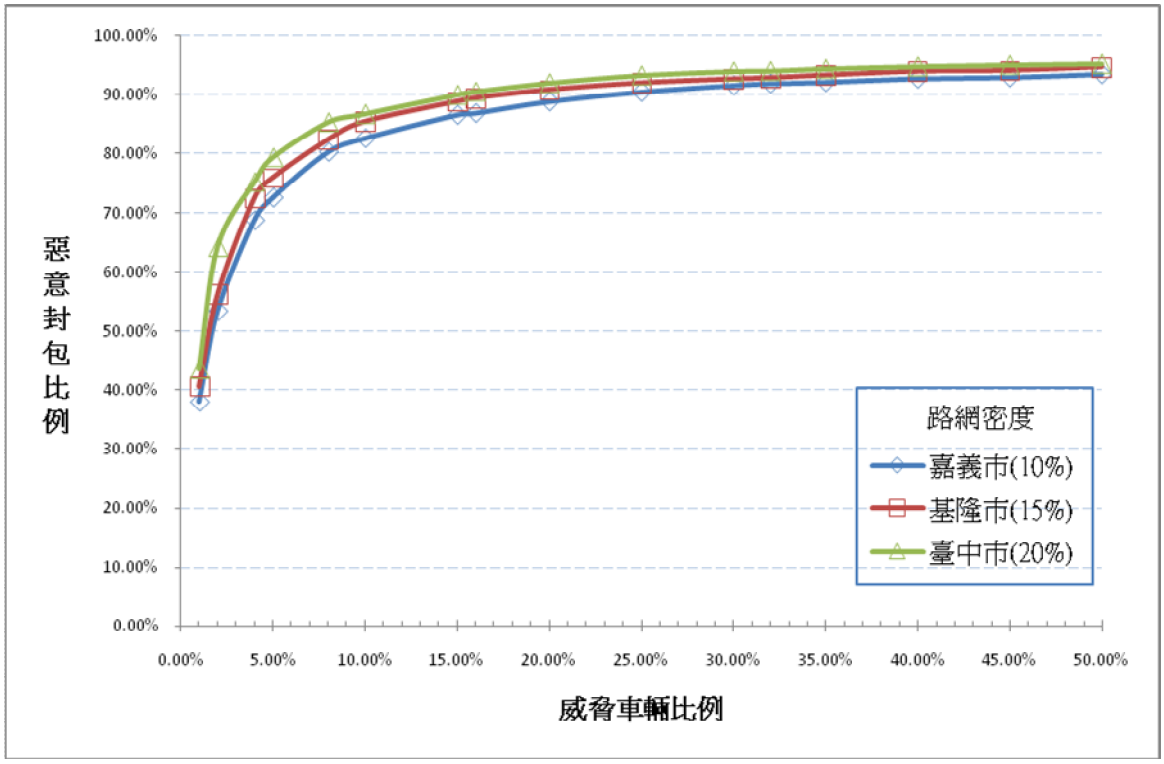
(a)最新時戳法則



(b)加權時戳法則



(c)地理+最新時戳法則



(d)地理+加權時戳法則

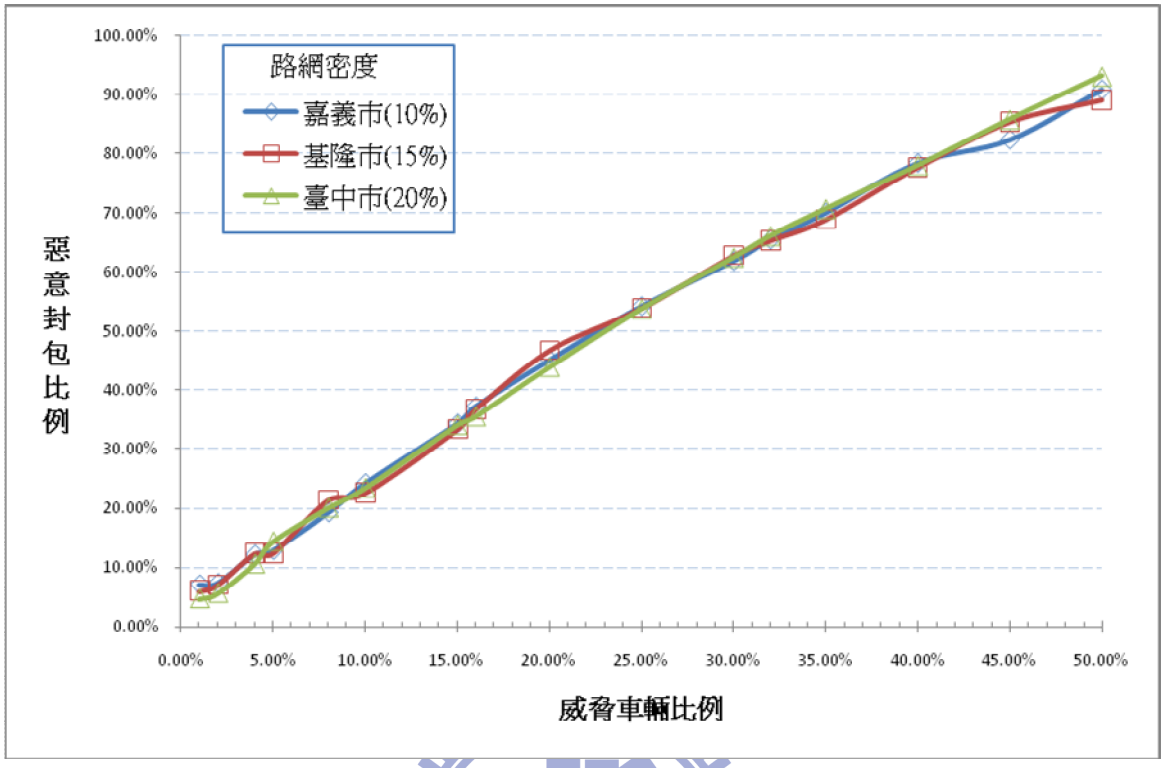
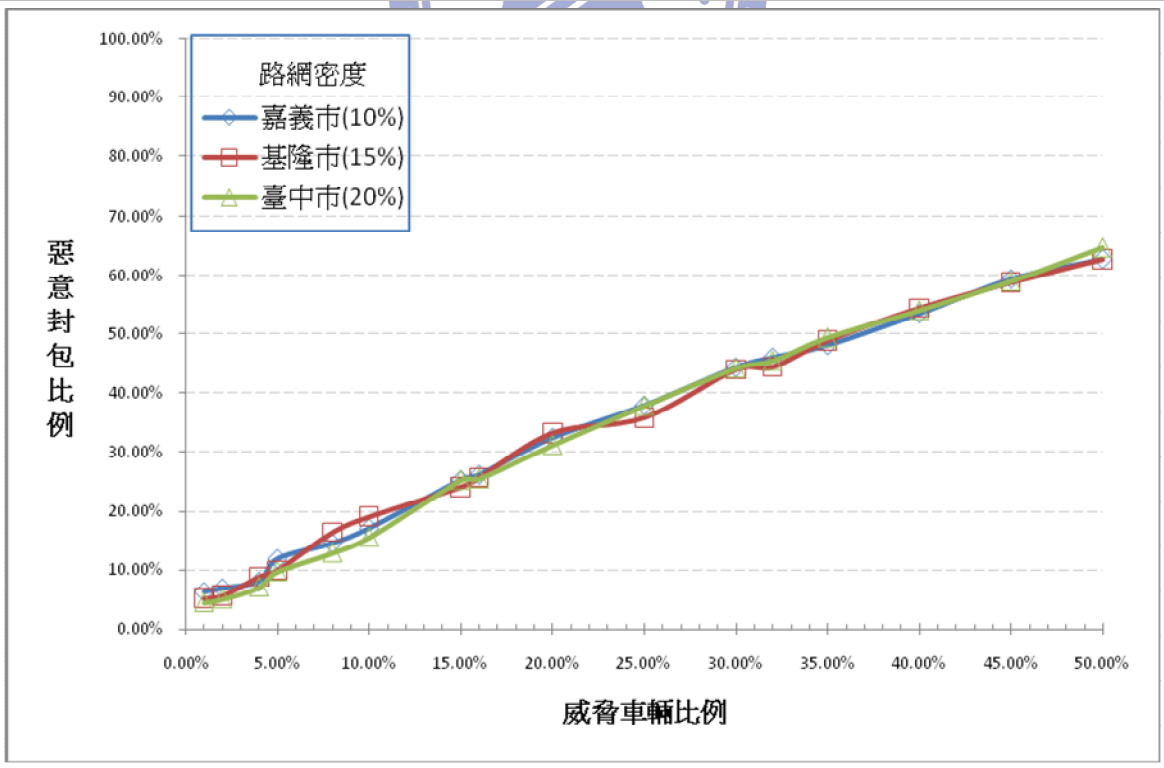
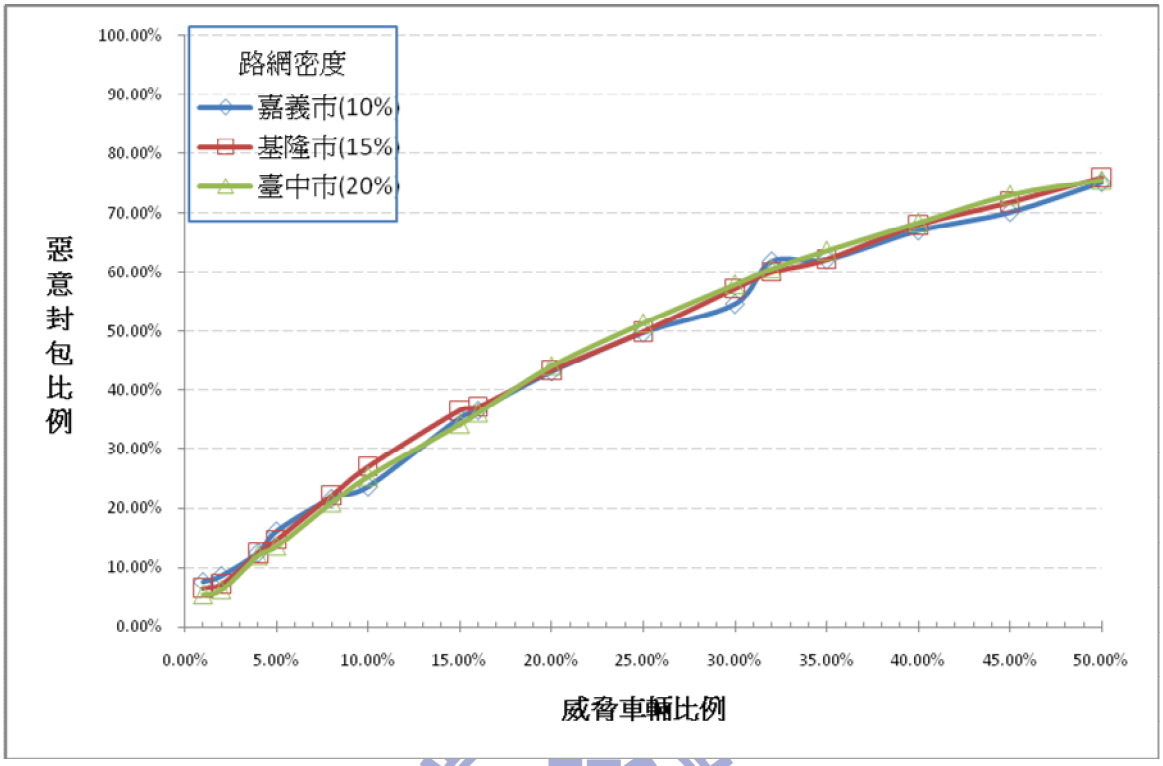


圖 4.1 考慮惡意訊息回向：路網密度對網路影響之分析

(a)偽造路況



(b)偽造路況和時戳



(c)考慮惡意訊息回向

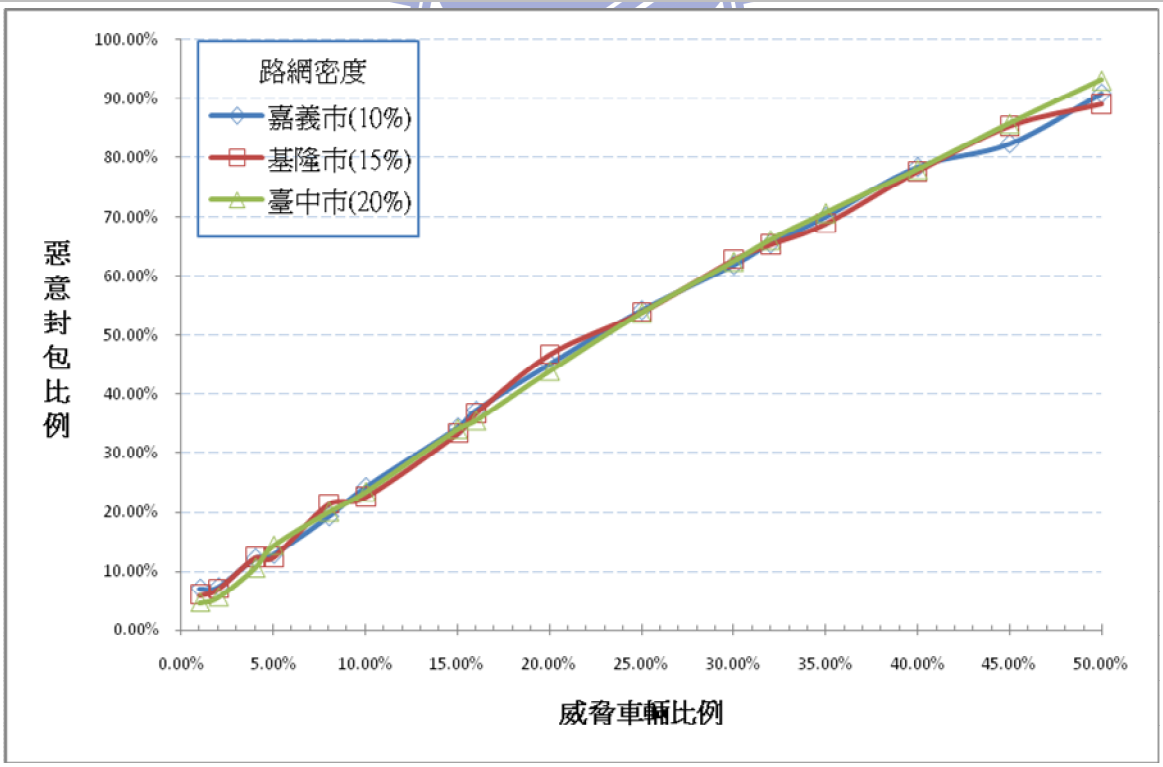


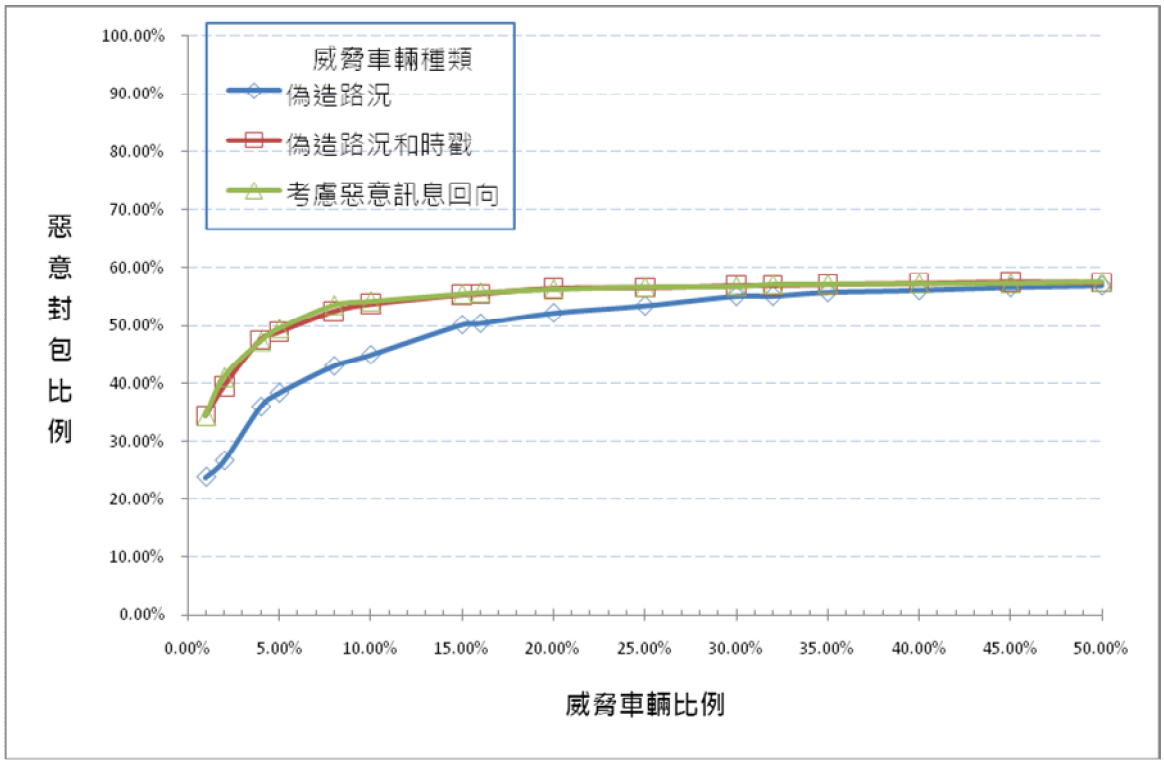
圖 4.2 地理+加權時戳法則：威脅車輛種類對網路影響之分析

圖 4.2 是地理+加權時戳法則路況更新方法在三種威脅車輛種類的比較。可以發現網路中的惡意封包比例在不同路網密度中，沒有多大的差別。參考附錄 A，也會發現另外三種路況更新方法在不同威脅車輛種類下，路網密度對惡意封包比例的影響並沒有很顯著。

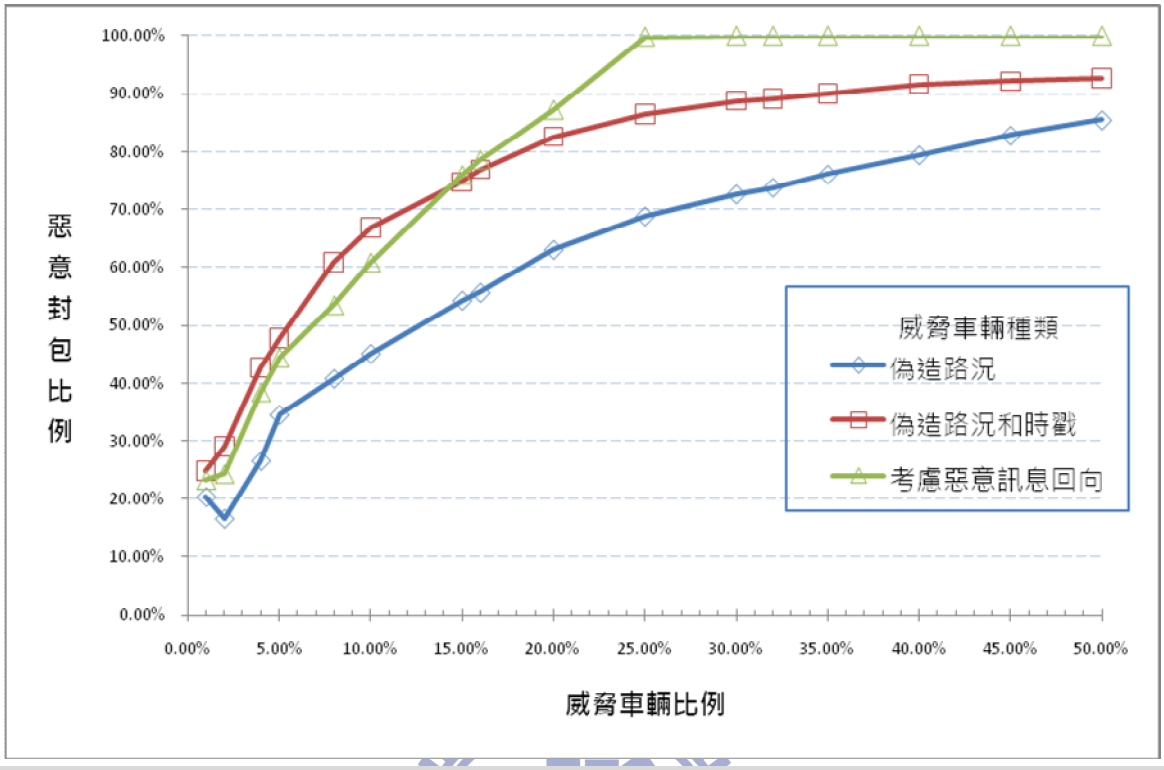
從上述可以得知，在四種路況更新方法和三種威脅車輛種類下，路網密度對網路中惡意封包比例沒有顯著的影響。

4.2.2 威脅車輛種類對網路影響之分析

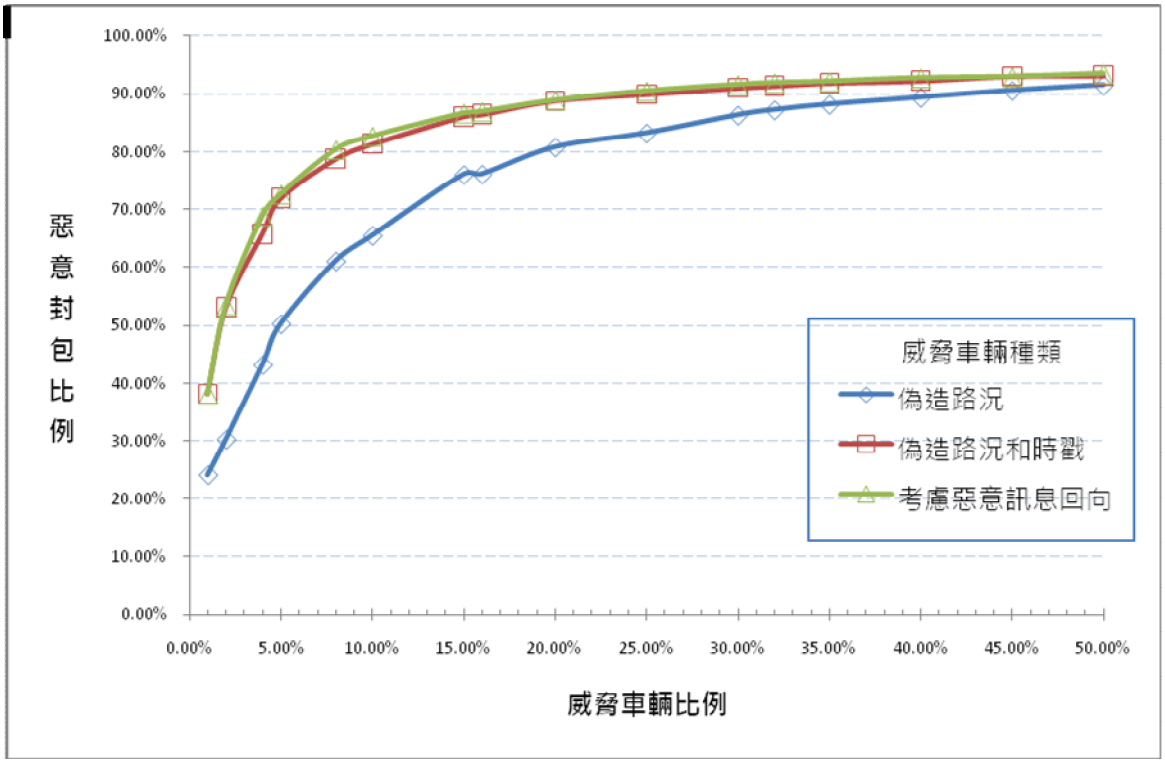
(a)最新時戳法則



(b)加權時戳法則



(c)地理+最新時戳法則



(d)地理+加權時戳法則

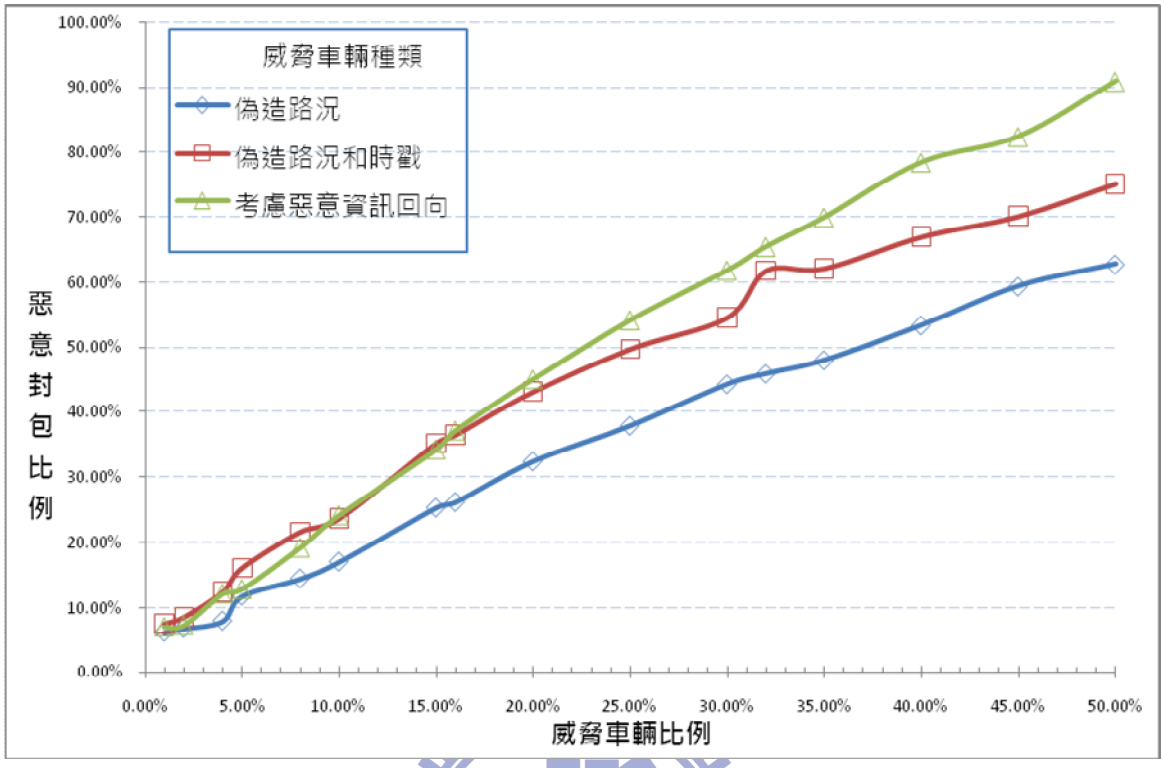


圖 4.3 嘉義市(10%)：威脅車輛種類對網路影響之分析

如圖 4.3，以嘉義市下班尖峰時刻為例。在四種路況更新方法中，偽造路況的威脅車輛對網路的影響最小。其餘兩種威脅車輛，在最新時戳法則和地理+最新時戳法則的路況更新方法下對網路的影響一樣大；在加權時戳法則和地理+加權時戳法則的路況更新方法下，在威脅車輛比例少時偽造路況和時戳的威脅車輛對路網影響最大，反之則是考慮惡意資訊回向的威脅車輛對網路影響最大。因為模擬會有誤差，發現在加權時戳法則的路況更新方法中，當威脅車輛比例超過 20%，還有地理+加權時戳法則的路況更新方法中，當威脅車輛比例超過 25%時，考慮惡意訊息回向的威脅車輛對網路的影響最大。

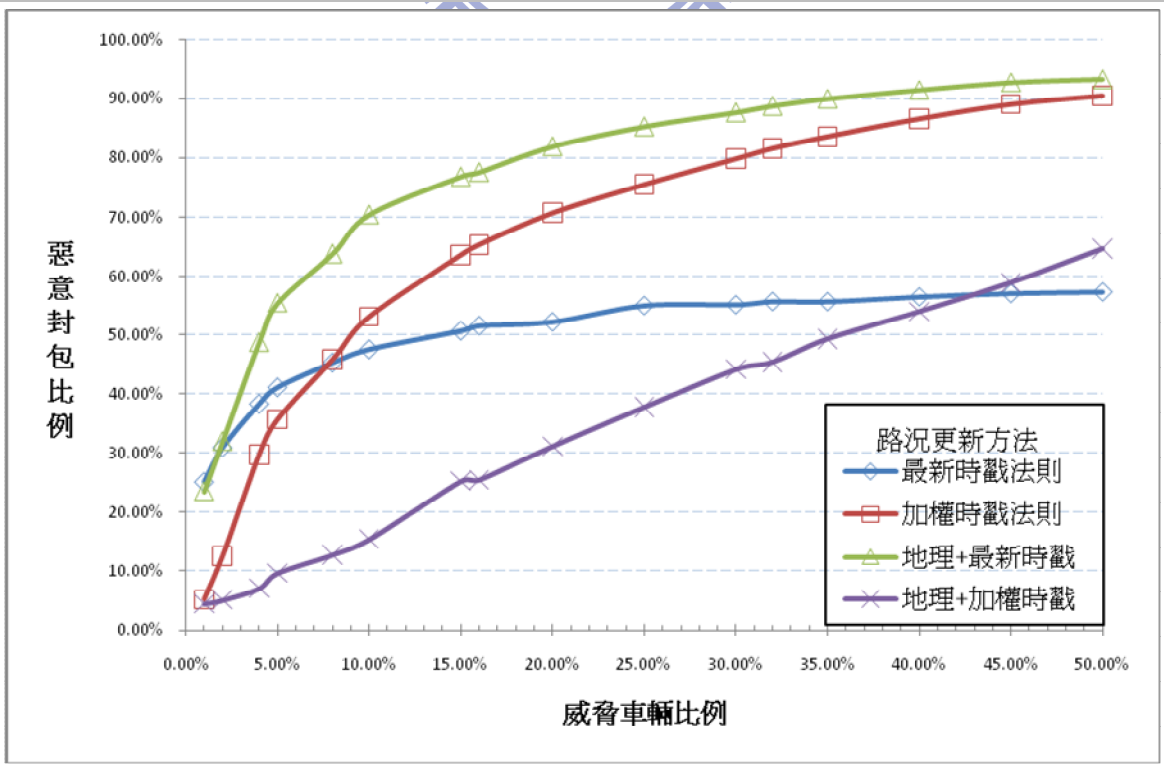
在某些情況下，考慮惡意訊息回向的威脅車輛對網路的影響最大，而其它狀況下，偽造路況和時戳的威脅車輛和考慮惡意訊息回向的威脅車輛對網路的影響一樣大。從整體而言，考慮惡意訊息回向的威脅車輛對網路的影響是最大的，對系統來說，如何有效抵抗考慮惡意訊息回向的威脅車輛帶來的干擾比較重要。因

此後面的實驗，主要針對考慮惡意訊息回向的威脅車輛為主來進行結果分析。

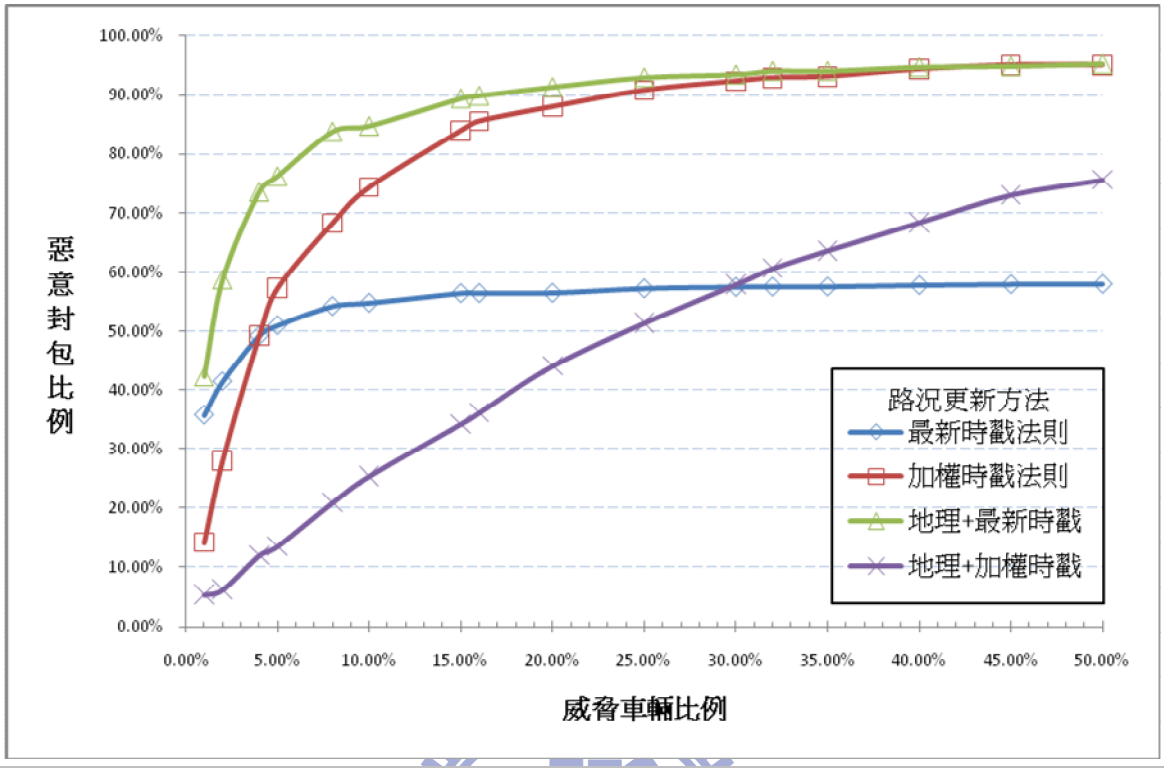
4.2.3 路況更新方法對網路影響之分析

圖 4.4 是以臺中市的下班尖峰時刻為例。在路網密度 20%、不同威脅車輛種類、不同威脅車輛比例以及不同的路況更新方法下進行的模擬。由圖可以看出，在三種威脅車輛中，一開始地理+加權時戳法則的路況更新方法最能有效抵抗惡意封包的干擾，但隨著威脅車輛比例的提高，都會在某個比例下，變成最新時戳法則的路況更新方法最能抵抗干擾。也可以發現當考慮地理相對位置後，地理+最新時戳法則的路況更新方法會比最新時戳法則的路況更新方法差；地理+加權時戳法則的路況更新方法會比加權時戳法則的路況更新方法佳。另外，發現在威脅車輛比例低時，考慮加權時戳法則的兩個路況更新方法都會比考慮最新時戳法則的兩個路況更新方法較佳。從以上所述，可以看出考慮地理相對位置無法絕對有效的抵抗惡意訊息的干擾。

(a)偽造路況



(b)偽造路況和時戳



(c)考慮惡意訊息回向

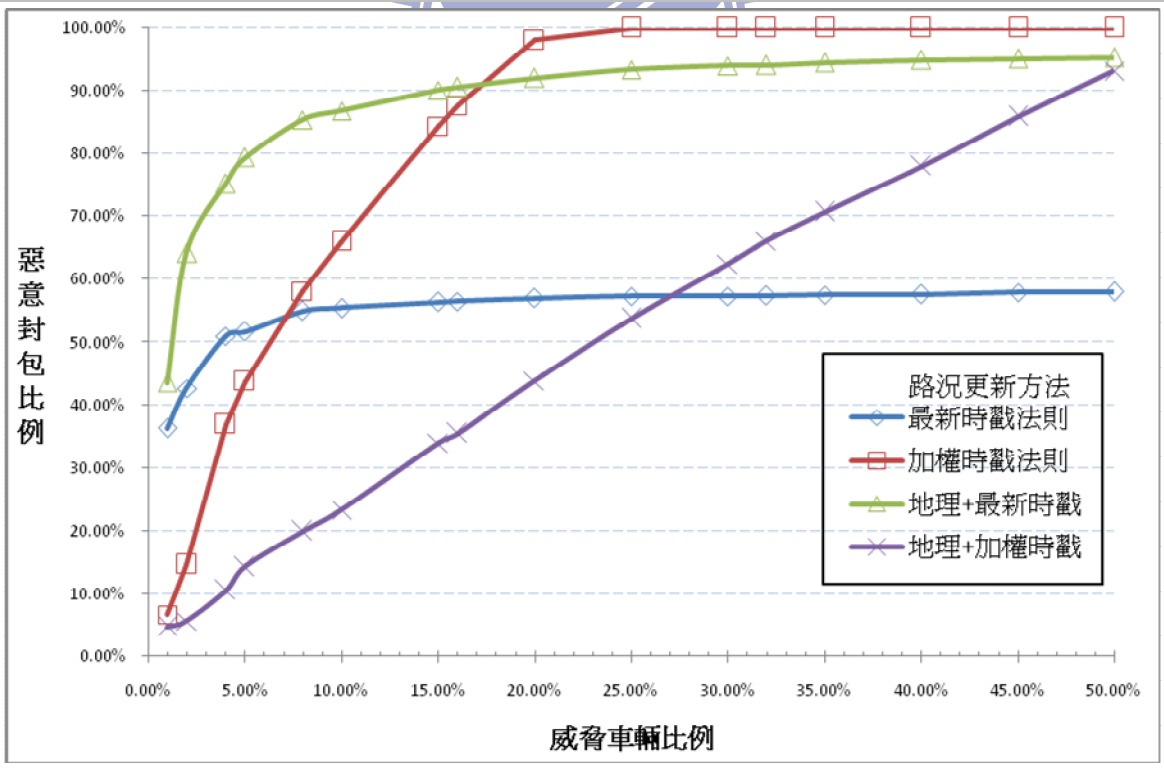


圖 4.4 臺中市(20%)：路況更新方法對網路影響之分析

綜合以上所述，可以發現在模擬中，網路中惡意封包的比例只會根據威脅車

輛的種類和不同的路況更新方法而有不同的變化，而路網密度對惡意封包的比例則影響不大。其中，考慮惡意訊息回向的威脅車輛對惡意封包比例的影響最大；而在威脅車輛比例低時，地理+加權時戳法則的路況更新方法最能抵抗惡意封包的干擾，反之，則是最新時戳法則的更新方法最佳。

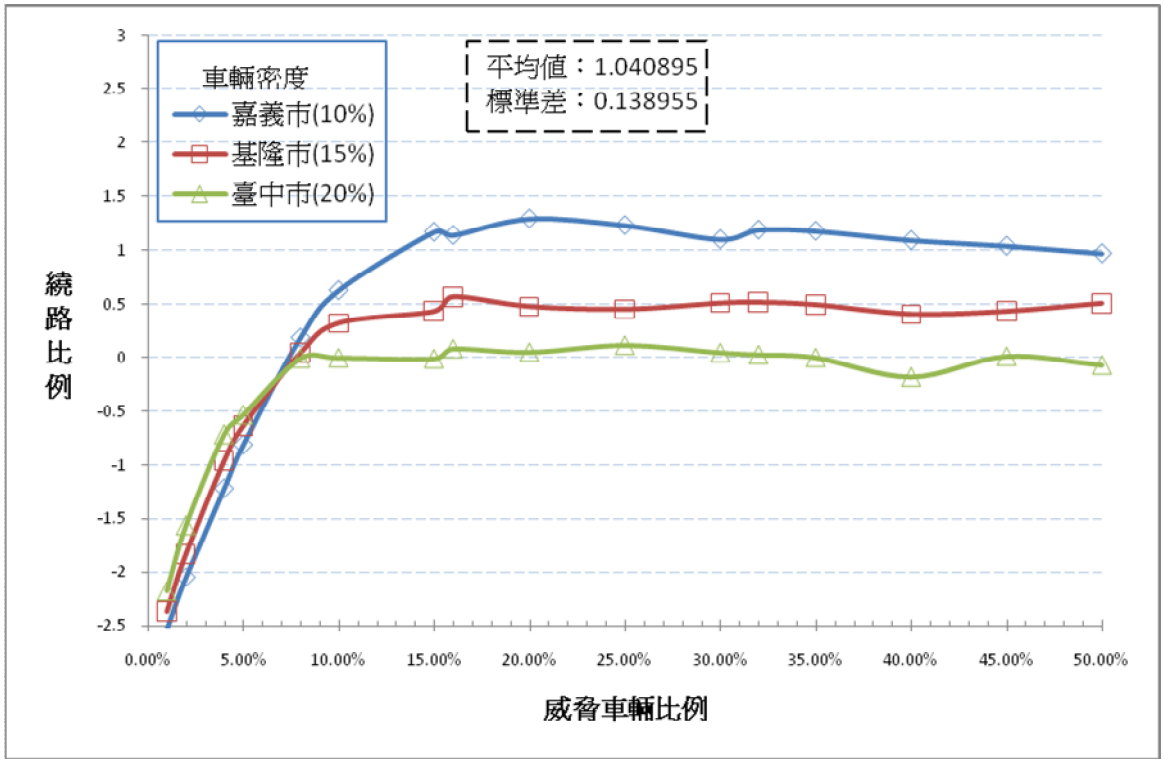
4.3 車輛效能之分析

在這個小節，主要是在不同的威脅車輛種類、不同的路況更新方法及不同的路網密度下，探討模擬得到的相關資料，如起點到目的地的最短距離、旅行時間、旅行距離，可以得到車輛的繞路比例和擁塞度，接著觀察在不同環境下繞路比例和擁塞度的變化關係。首先，會先觀察在不同的路網密度下，車輛的繞路比例和擁塞度之間會有什麼關係和變化；接著會在不同環境、不同的路況更新方法下，觀察繞路比例和擁塞度會有什麼影響及變化。

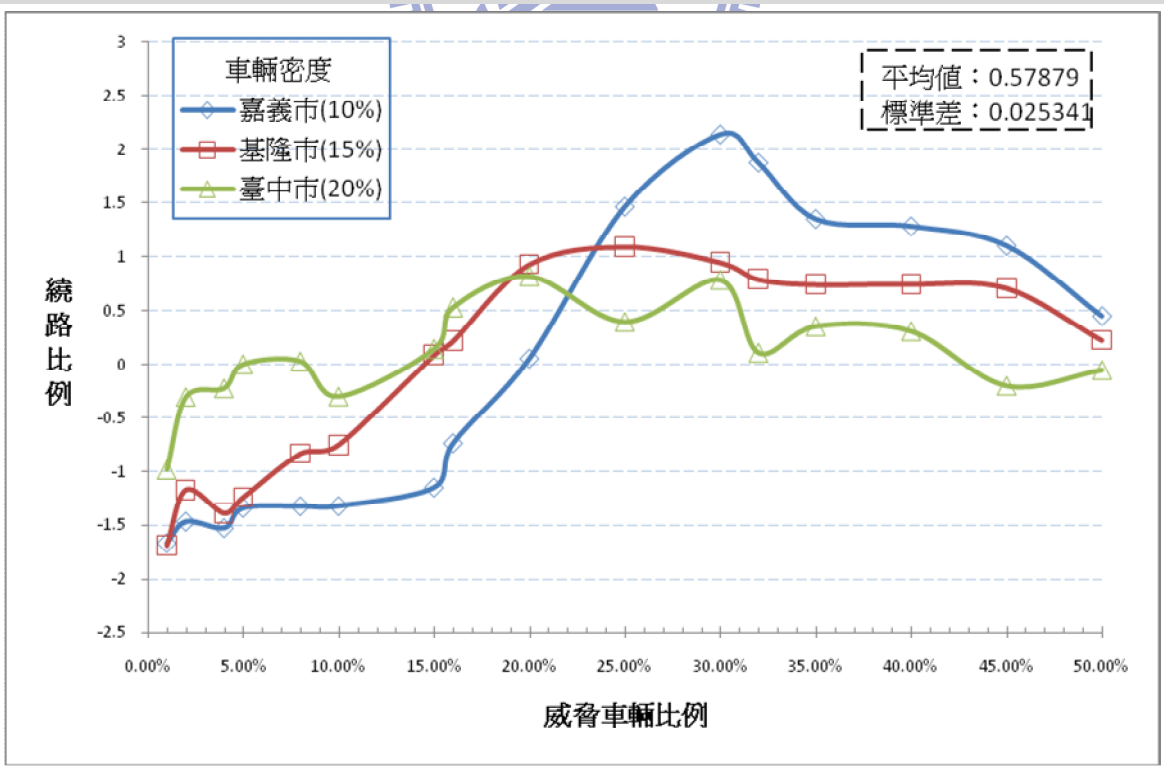
4.3.1 路網密度對效能影響之分析

圖 4.5 是在考慮惡意訊息回向的威脅車輛下，在不同的路網密度、不同路況更新方法以及不同威脅車輛比例所進行的模擬結果。從圖中可以發現，在威脅車輛比例低時，路網密度低的繞路比例相對的比較少；反之，當威脅車輛比例高時，路網密度高的繞路比例相對的比較少。從整體而言，最新時戳法則和地理+最新時戳法則的路況更新方法，在路網密度高時，多跑距離比例會最少；加權時戳法則的路況更新方法則是在威脅車輛比例低於 22%時，路網密度低的效能較佳，當威脅車輛比例超過 22%時，路網密度高的效能較佳；地理+加權時戳法則的路況更新方法則是路網密度低的繞路比例會最少。參考附錄 B，偽造路況和偽造路況和時戳這兩種威脅車輛，也會和考慮惡意訊息回向的威脅車輛有相同的模擬結果。

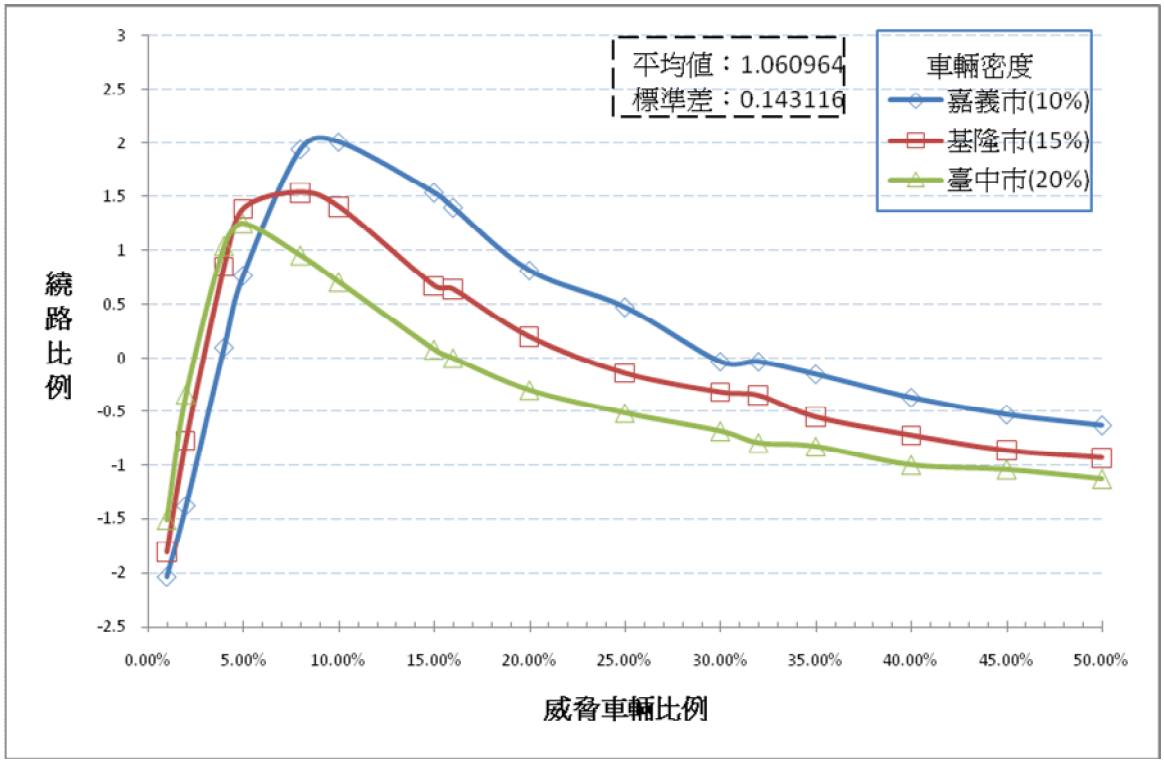
(a)最新時戳法則



(b)加權時戳法則



(c)地理+最新時戳法則



(d)地理+加權時戳法則

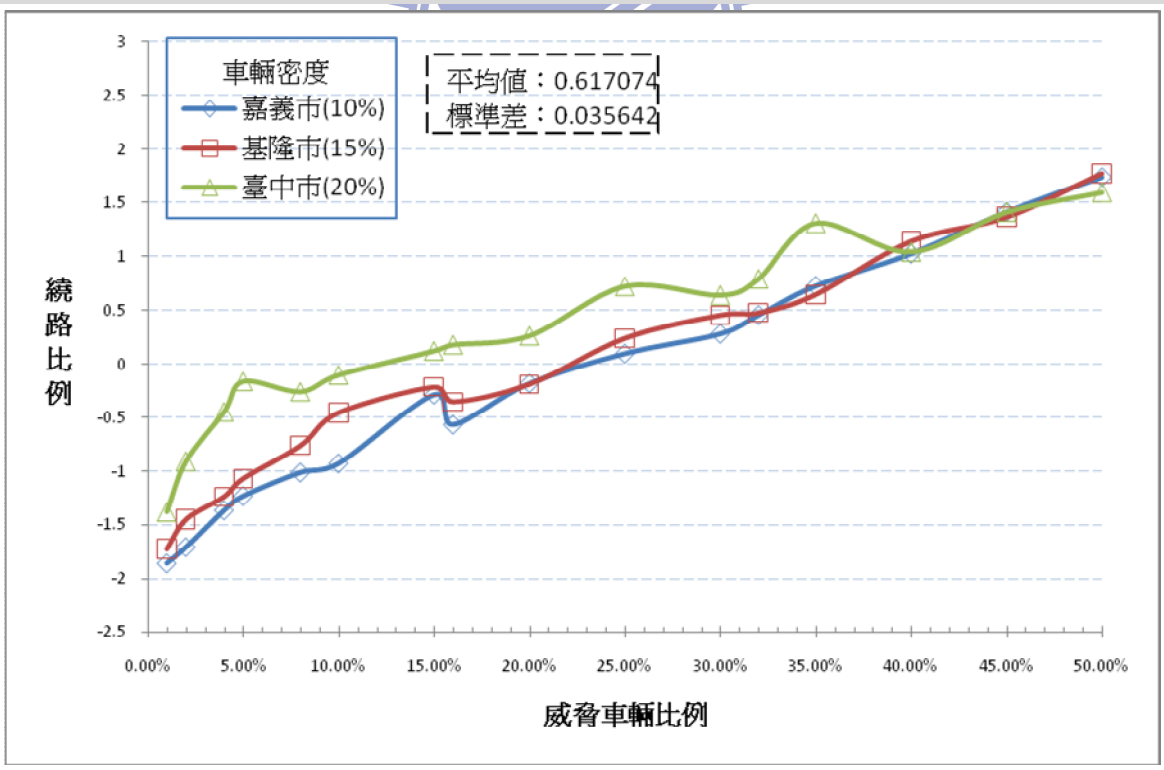
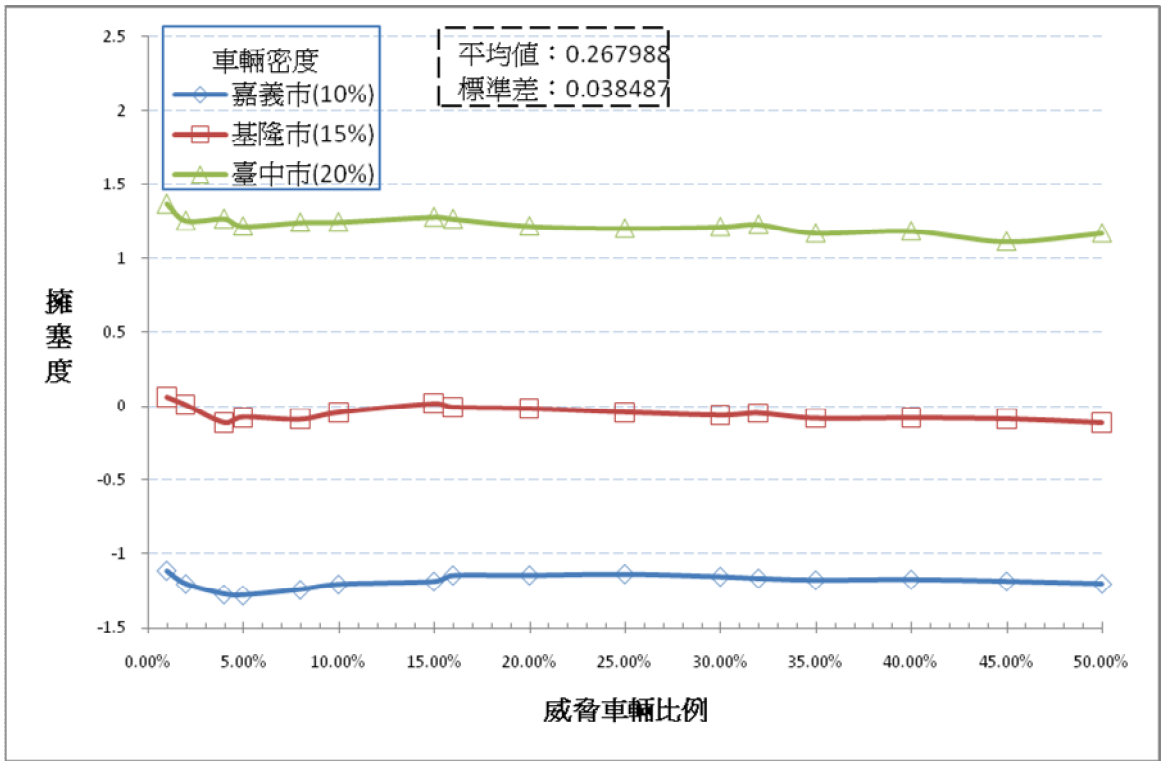


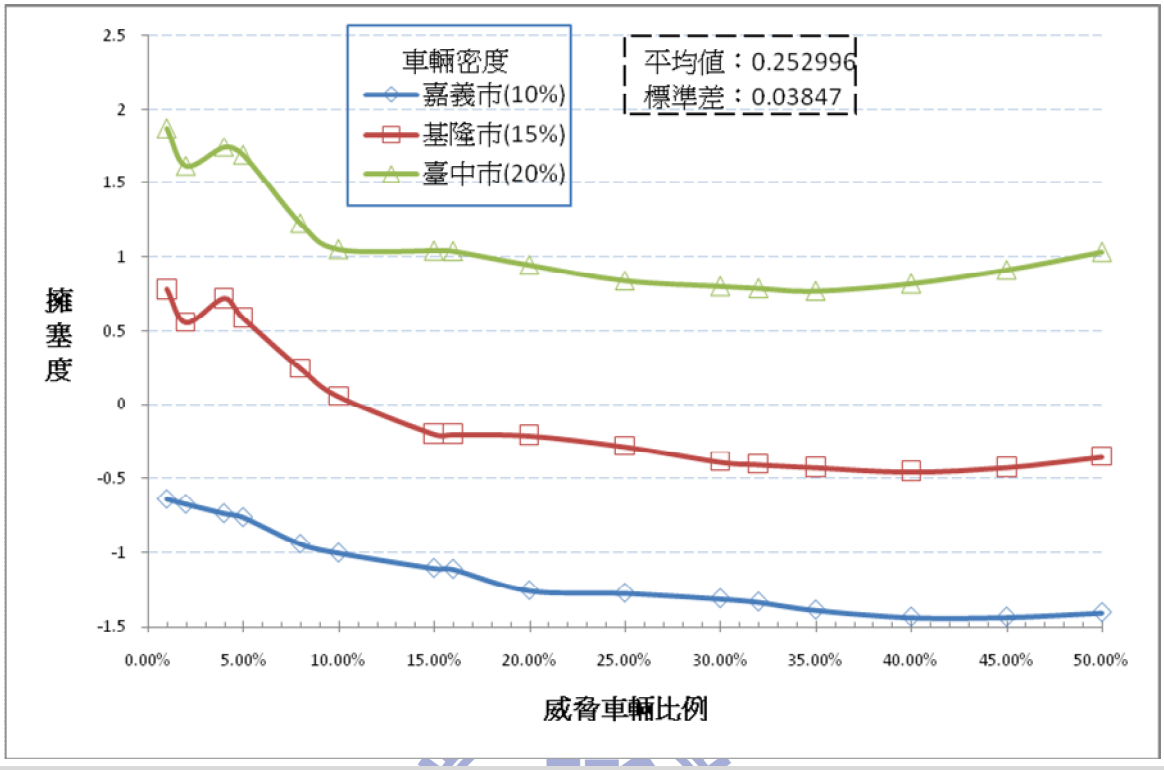
圖 4.5 考慮惡意訊息回向：路網密度對繞路比例影響之分析

圖 4.6 主要是針對考慮惡意訊息回向的威脅車輛，在不同的車輛密度、不同威脅車輛比例以及不同的路況更新方法進行的模擬結果。可以發現在四種路況更新的方法下，隨著車輛密度的提高，效能也會隨之下降。這就好比郊區和上下班的尖峰時刻，郊區的車輛密度小，車輛幾乎都可以全速的行駛在道路上，而在都市中，特別是上下班的尖峰時刻，車輛密度很高，車流幾乎都是走走停停的，效能明顯的會比郊區的車輛還要差。

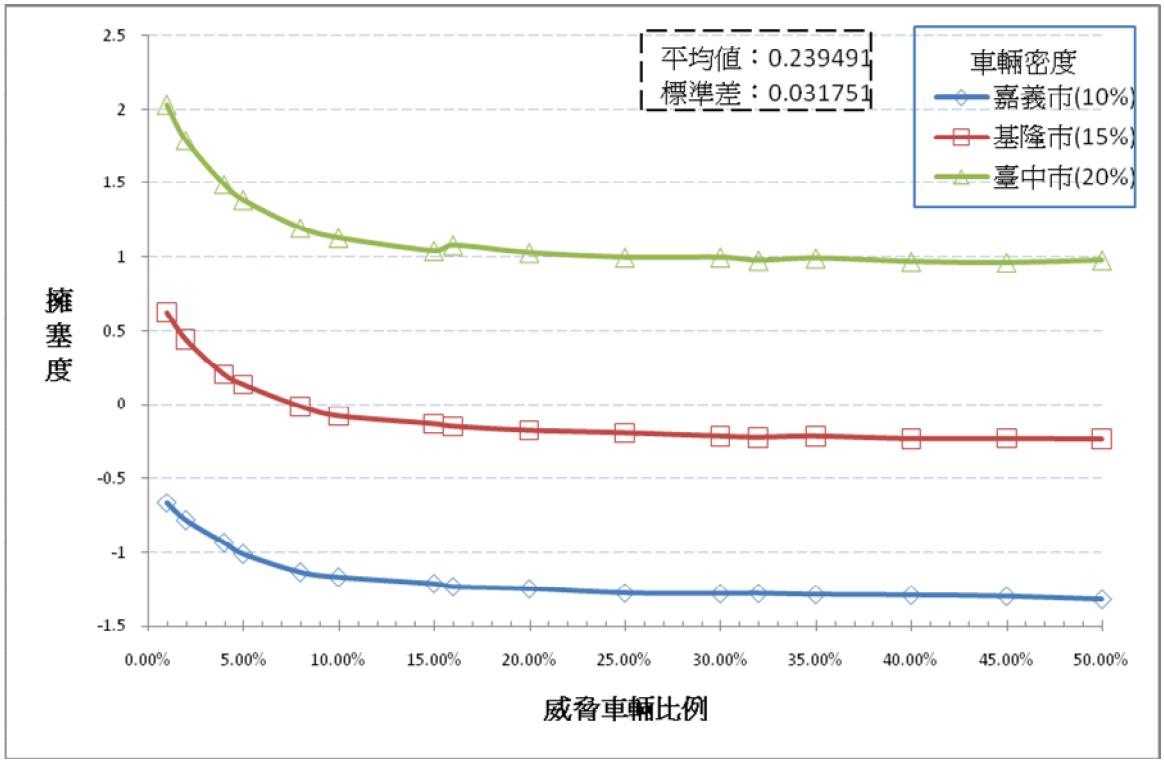
(a)最新時戳法則



(b)加權時戳法則



(c)地理+最新時戳法則



(d)地理+加權時戳法則

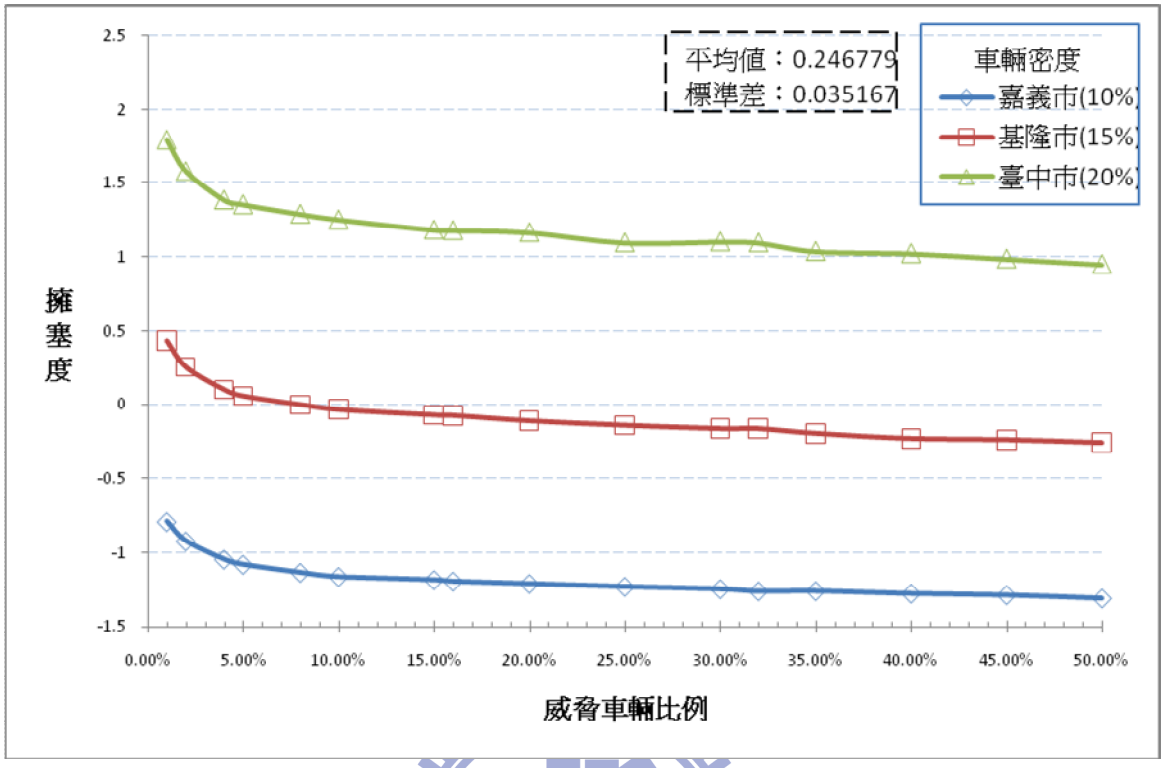


圖 4.6 考慮惡意訊息回向：路網密度對擁塞度影響之分析

從上述可知，路網密度對繞路比例的影響會根據使用的路況更新方法不同而有不同的結果；對擁塞度的影響則是在各種路況更新方法下，皆會隨著路網密度的升高而使得效能降低。

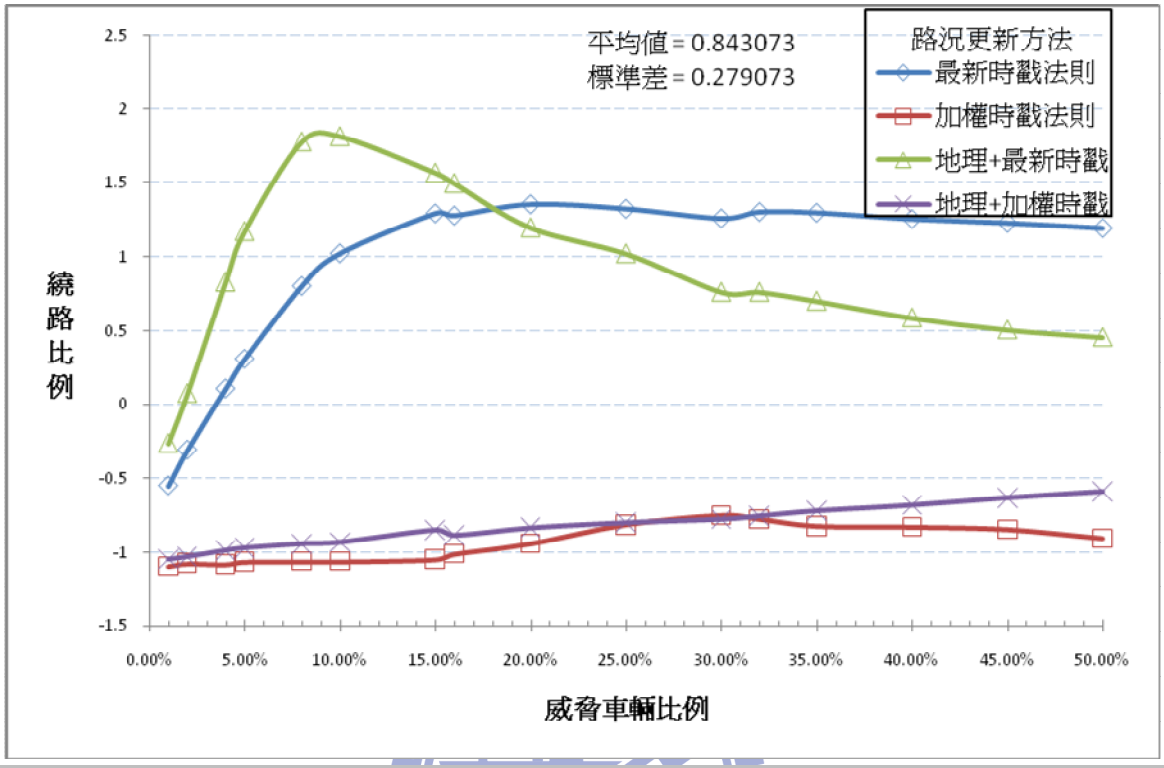
4.3.2 繞路比例分析

圖 4.7 主要是針對考慮惡意訊息回向的威脅車輛，在不同的路網密度、不同的路況更新方法、不同的威脅車輛比例下進行的模擬結果。可以發現加權時戳法則的路況更新方法繞路比例明顯的最少；接著地理+加權時戳法則的路況更新方法效能次之；而在威脅車輛比例 18%之前，地理+最新時戳法則的路況更新方法繞路比例最差，當威脅車輛比例超過 18%之後，最新時戳法則的路況更新方法繞路比例最差。參考附錄 C，可以發現在另外兩種威脅車輛種類下，除了在路網密度低時，修改權重的威脅車輛種類一直是地理+最新時戳法則的路況更新方法最差不同外，其餘模擬得到的結果跟考慮惡意訊息回向的威脅車輛一樣。

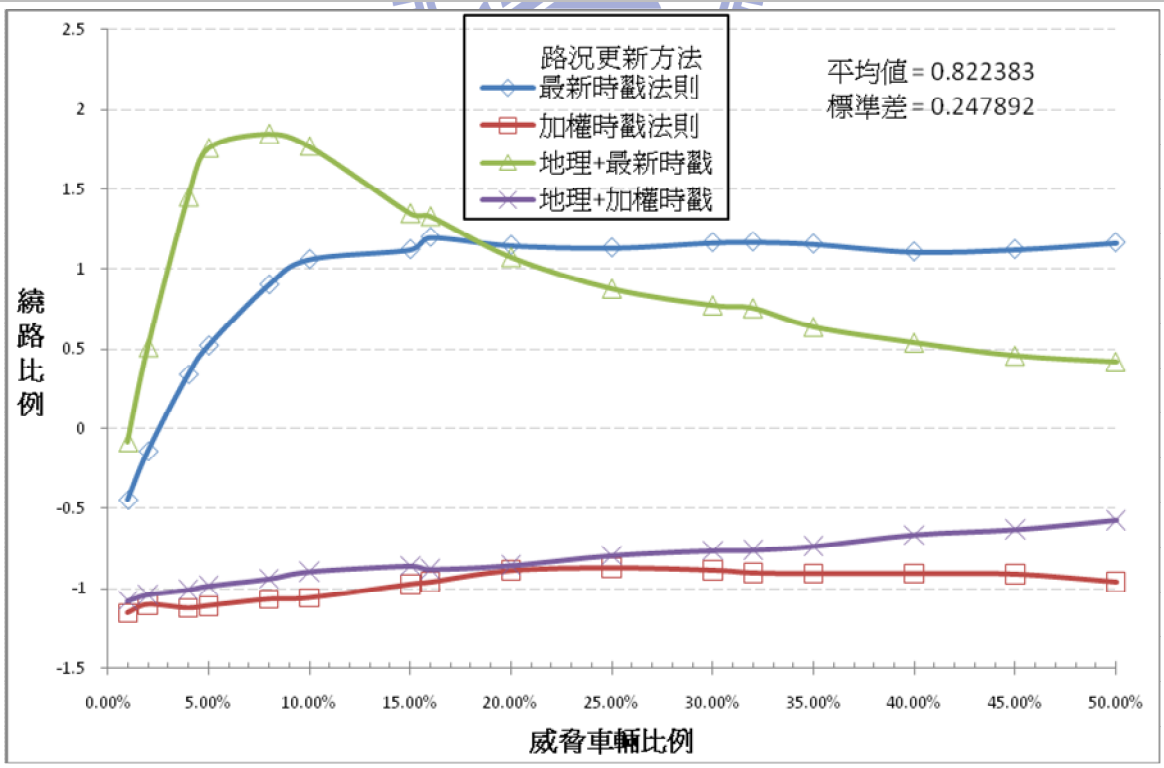
從大部分的情況而言，可以得到一個明顯的結果。在繞路比例的比較，加權時戳法則的路況更新方法最佳，地理+加權時戳法則的路況更新方法次佳，地理+最新時戳法則的路況更新方法次糟，最新時戳法則的路況更新方法最糟。可以看出，當使用加權時戳法則為主的路況更新方法會比使用最新時戳法則為主的路況更新方法在繞路比例有較佳的效能。

從駕駛者的角度來看，加權時戳法則的路況更新方法效能最佳，能讓多跑的距離明顯的最少。而多跑距離的多寡，也跟耗油程度有直接的關聯，因此加權時戳法則的路況更新方法也可說是最省油的路況更新方法。

(a)嘉義市(10%)



(b)基隆市(15%)



(c)臺中市(20%)

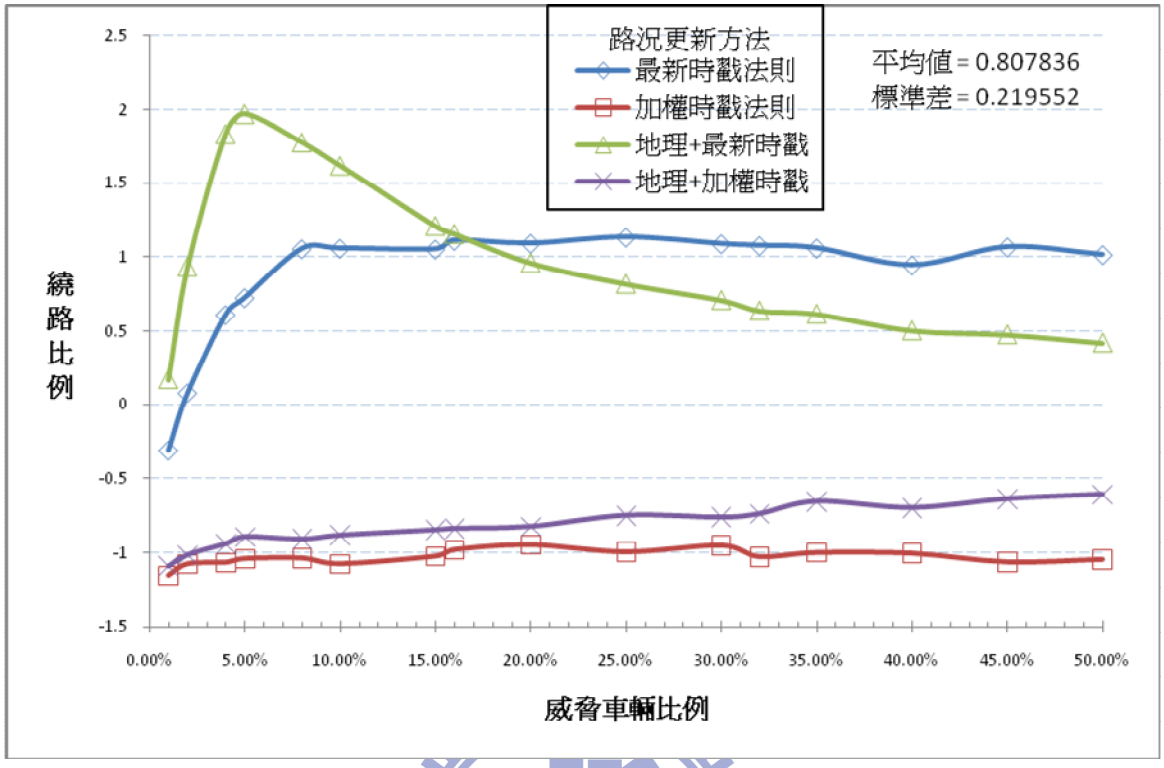
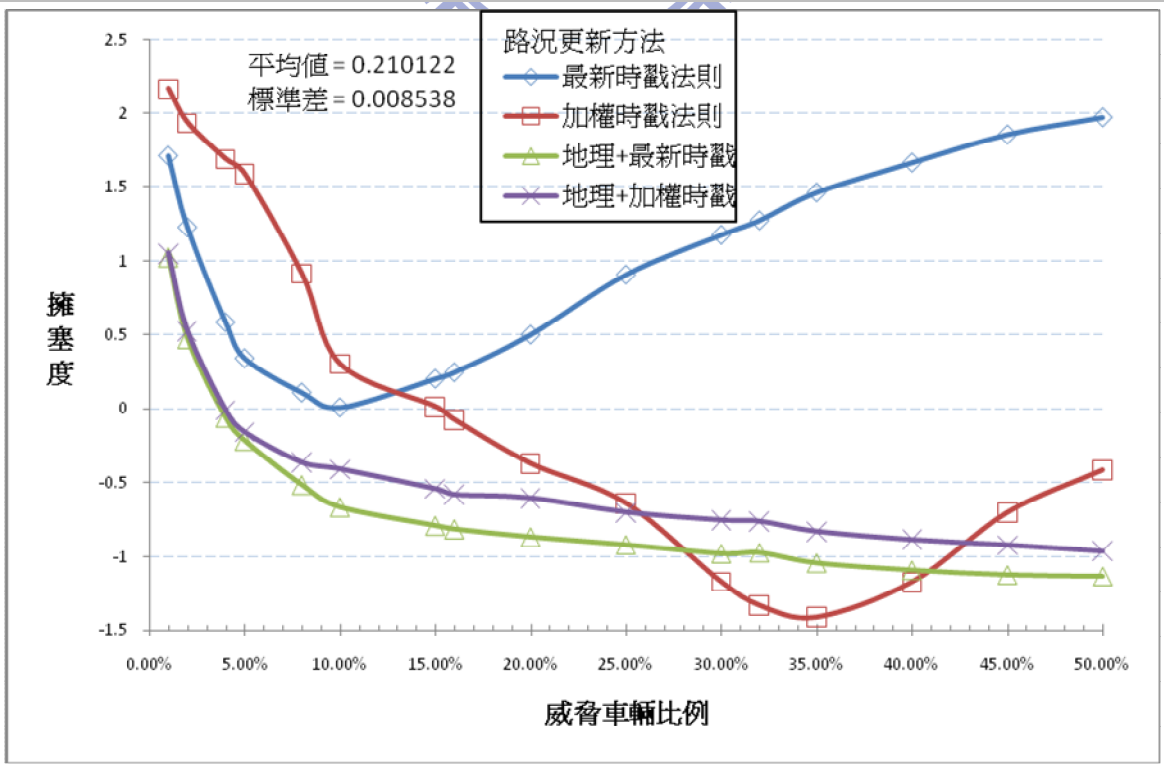


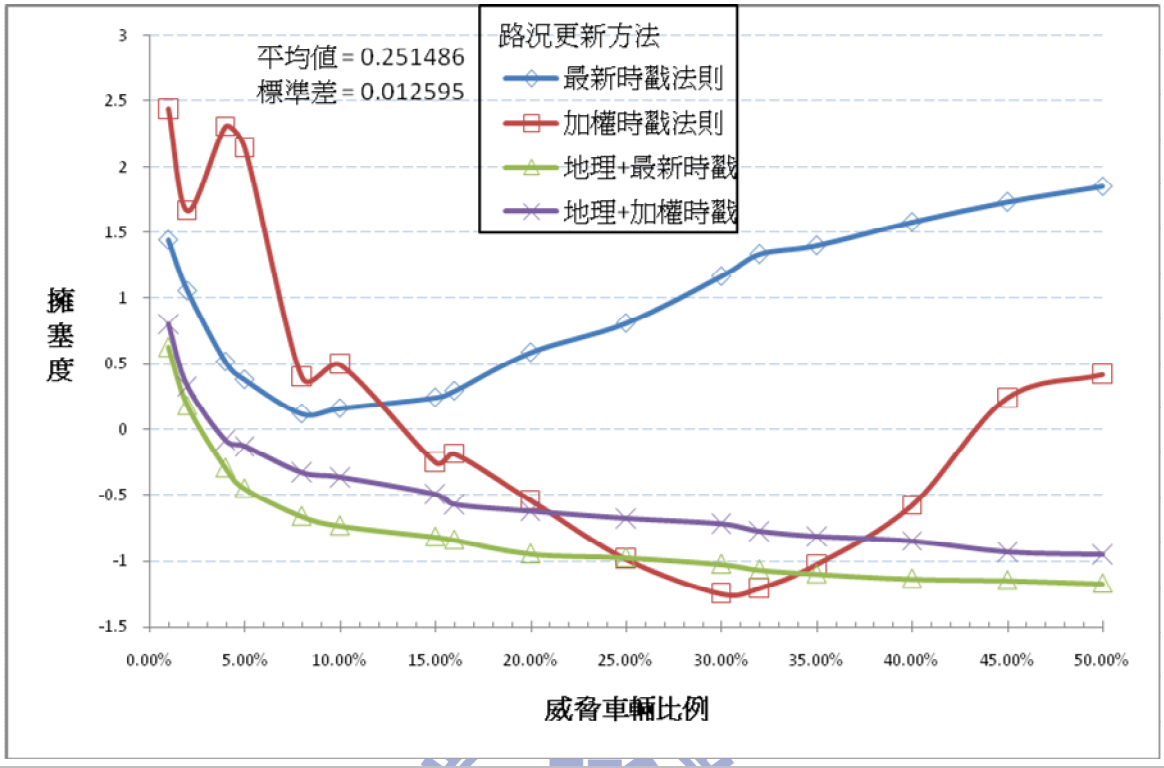
圖 4.7 考慮惡意訊息回向：路況更新方法對繞路比例影響之分析

4.3.3 擁塞度分析

(a)嘉義市(10%)



(b)基隆市(15%)



(c)臺中市(20%)

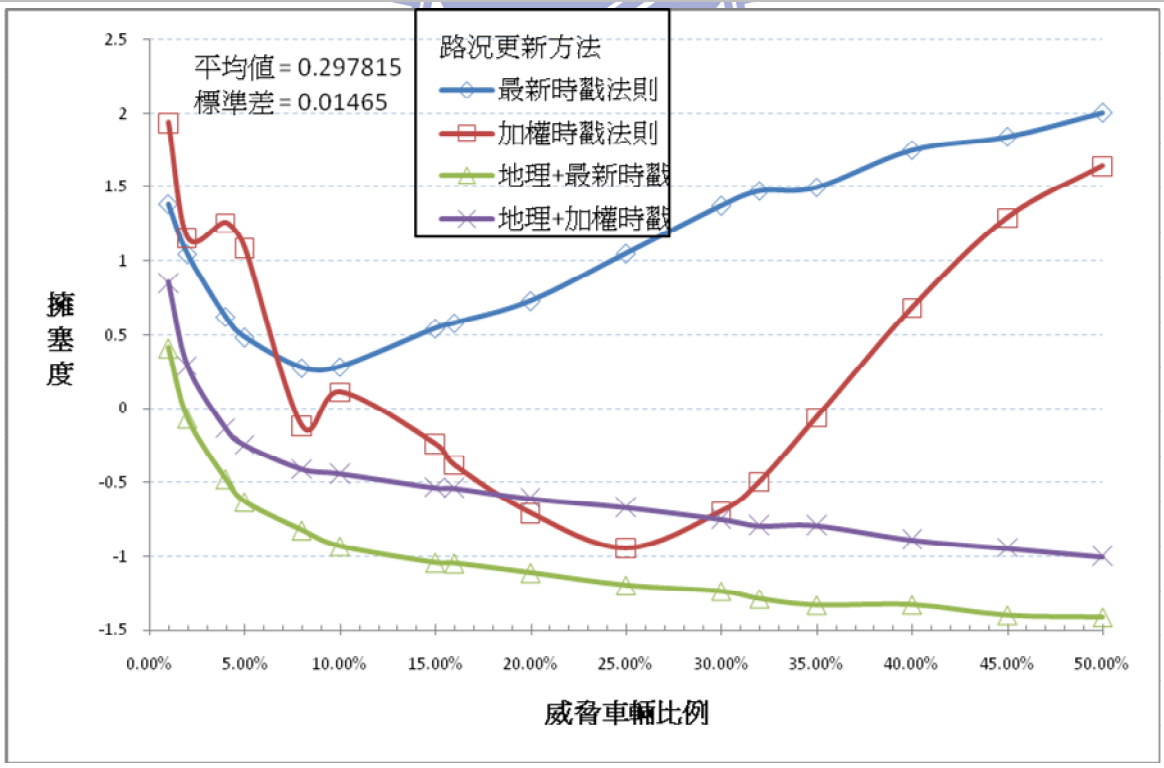
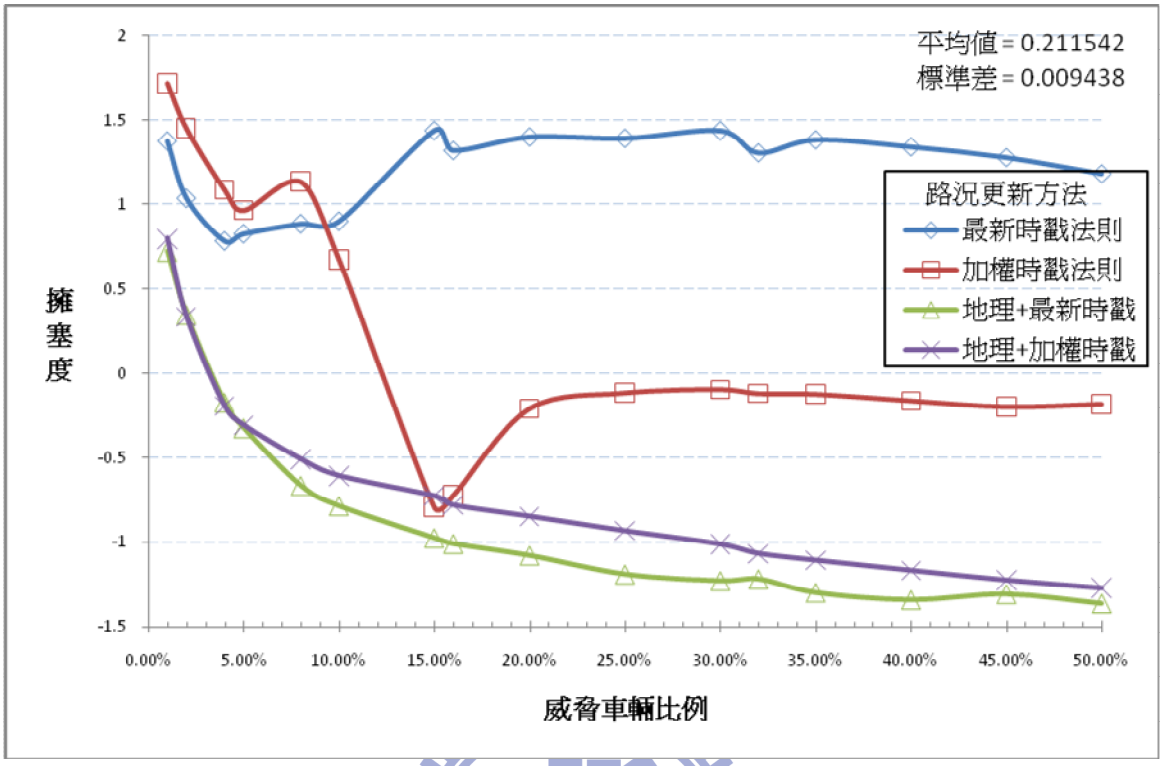
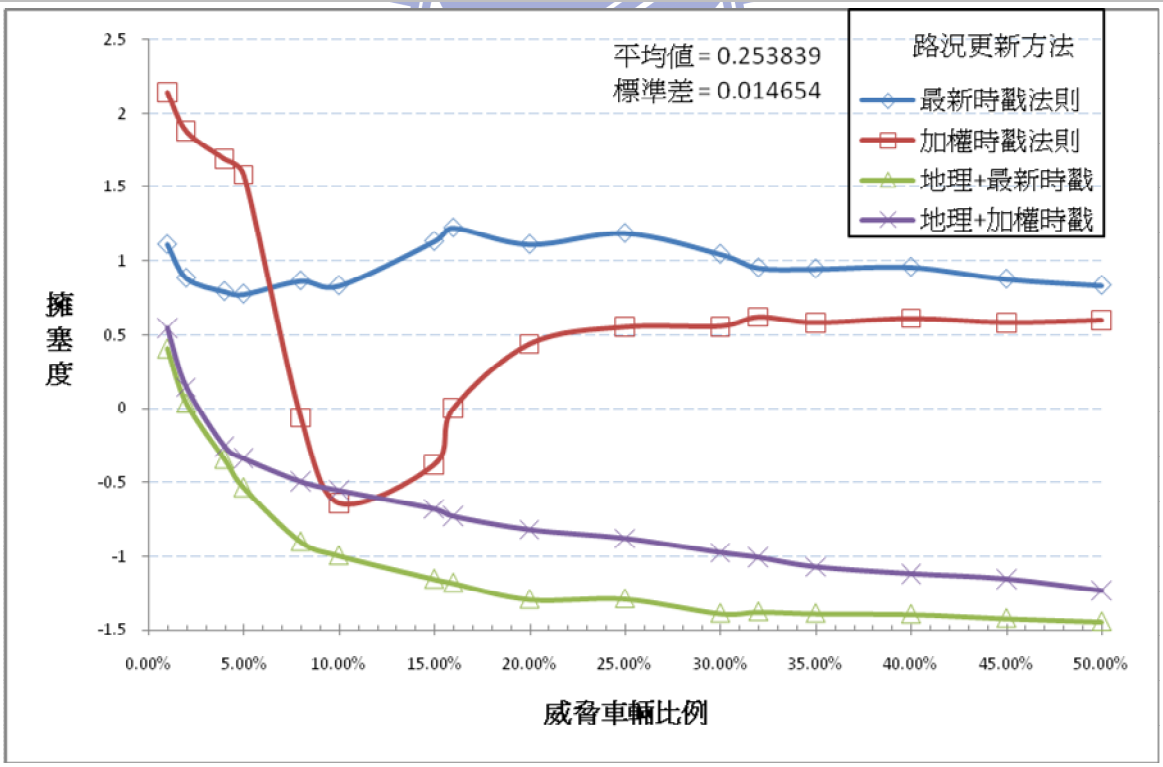


圖 4.8 偽造路況：路況更新方法對擁塞度影響之分析

(a)嘉義市(10%)



(b)基隆市(15%)



(c)臺中市(20%)

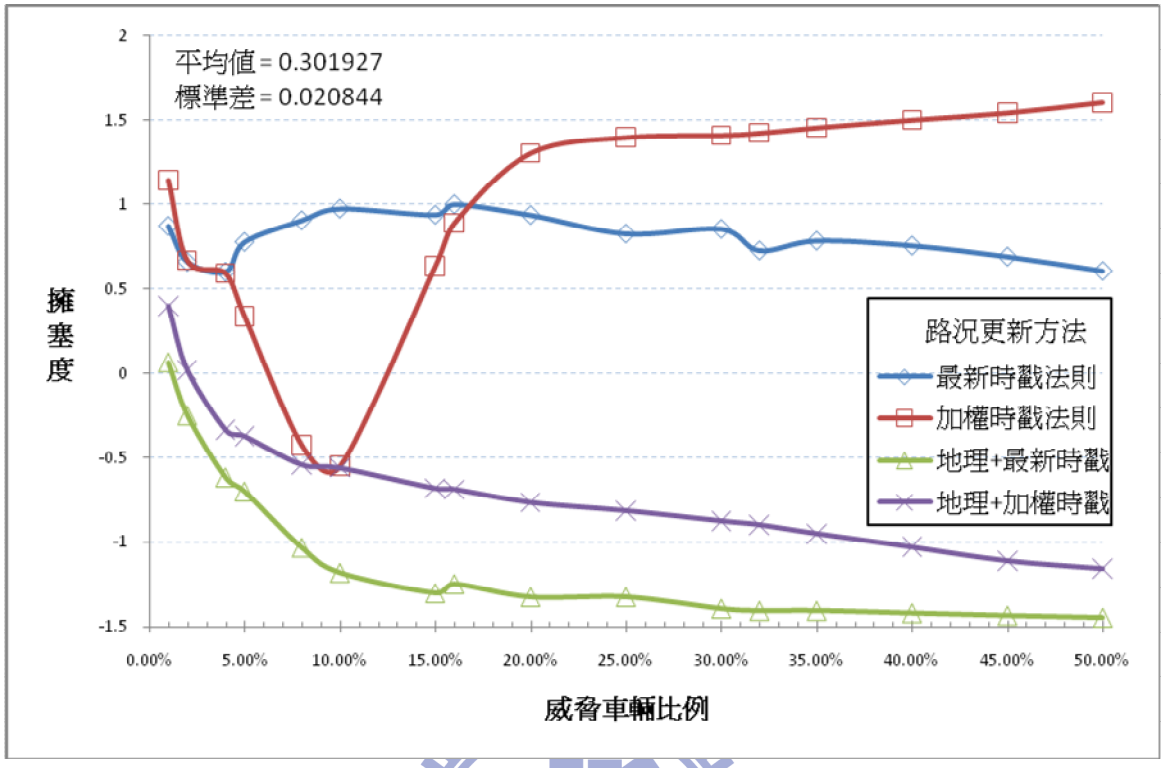
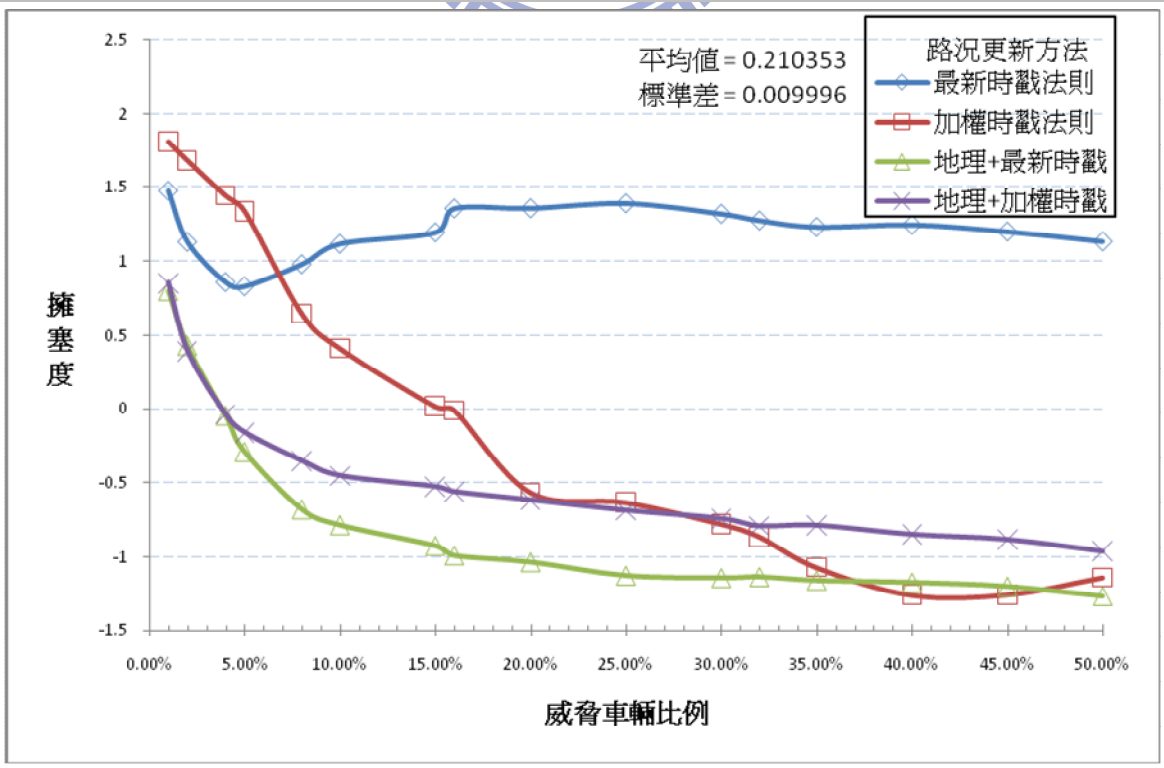
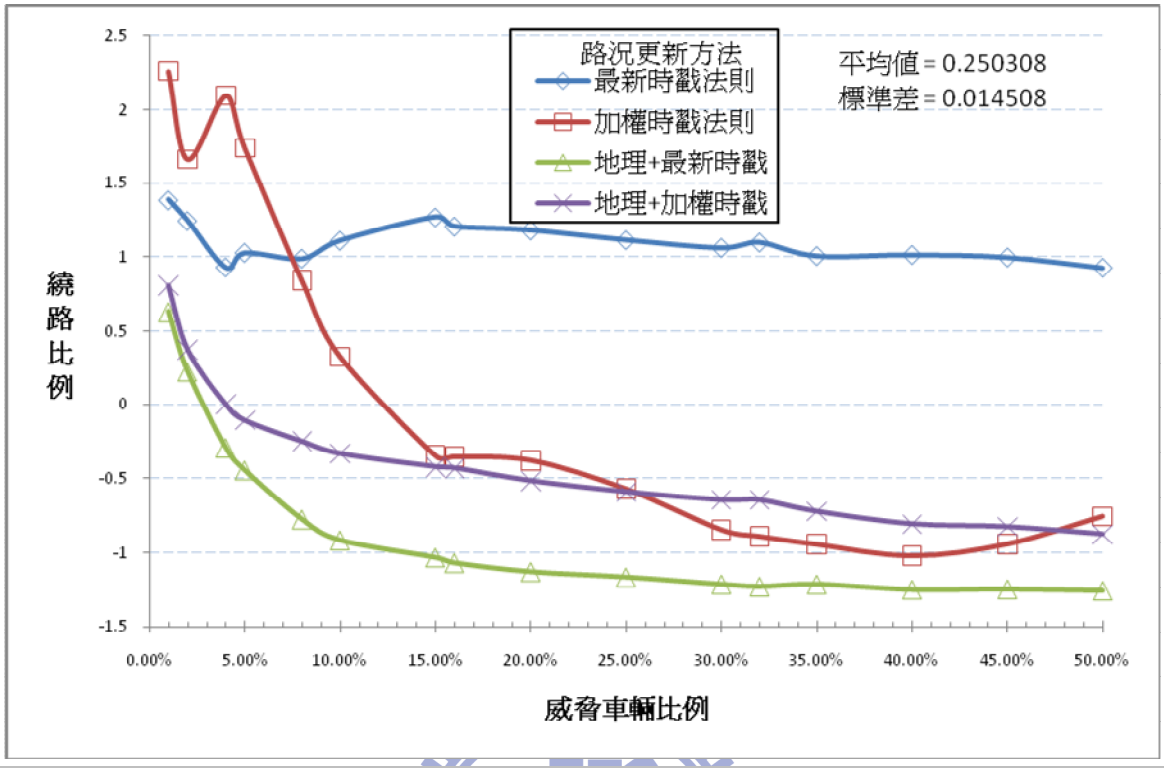


圖 4.9 偽造路況和時戳：路況更新方法對擁塞度影響之分析

(a)嘉義市(10%)



(b)基隆市(15%)



(c)臺中市(20%)

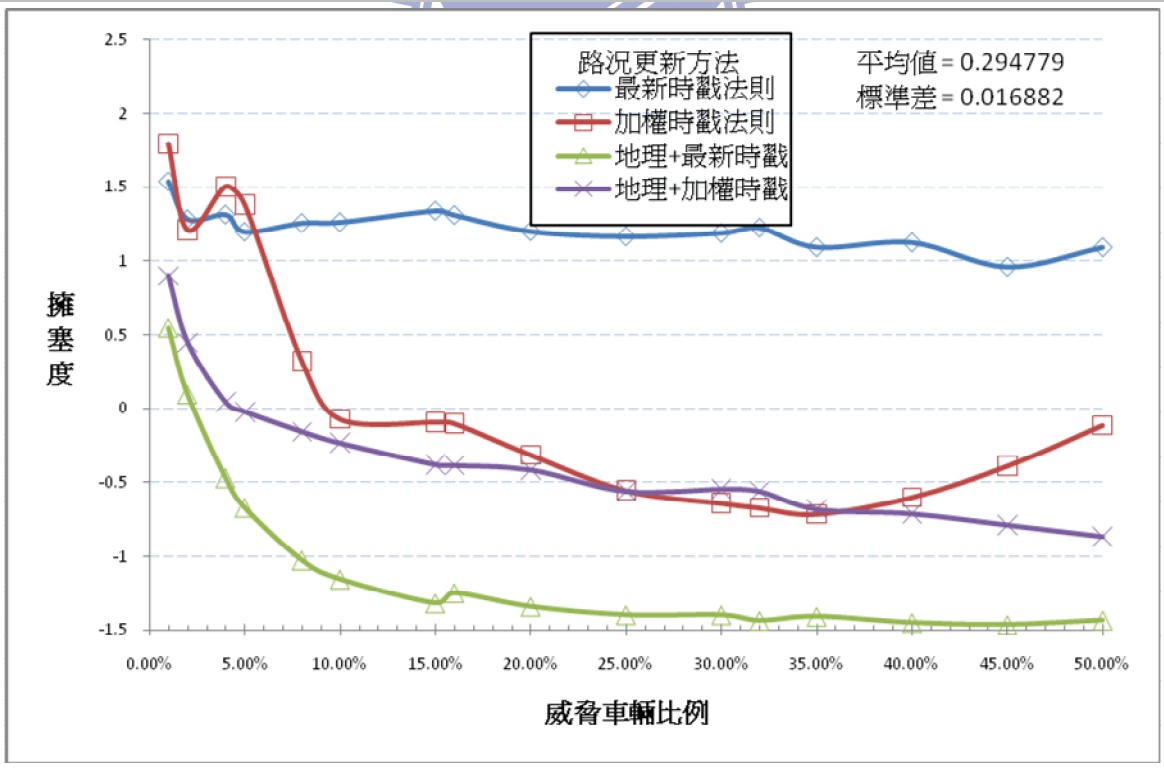


圖 4.10 考慮惡意訊息回向：路況更新方法對擁塞度影響之分析

圖 4.8、圖 4.9 和圖 4.10 是分別在偽造路況、偽造路況和時戳以及考慮惡

意訊息回向的威脅車輛種類下，對不同威脅車輛比例、不同路況更新方法、不同路網密度進行模擬得到的結果。從圖可以明顯得知，加權時戳法則的路況更新方法會依環境的不同而有不同的結果。另外三種路況更新方法之間對於擁塞度的效能優劣，則是地理+最新時戳法則的路況更新方法最佳，地理+加權時戳法則的路況更新方法次佳，最新時戳法則的路況更新方法最差。

從圖可以發現，加權時戳法則的路況更新方法受路網密度的影響最大。密度只要稍微變化，擁塞度的變化就很大。在偽造路況的威脅車輛環境下，在路網密度高時，最後擁塞度的效能次糟，但很逼近最新時戳法則路況更新方法的擁塞度；在偽造路況和時戳的威脅車輛環境下，路網密度低時，擁塞度的效能次糟，但路網密度一旦提高，擁塞度的效能會明顯的降低，最後變成最糟的狀況；而在考慮惡意訊息回向的威脅車輛環境下，加權時戳法則的路況更新方法擁塞度效能受路網密度的影響相對的比較小，不過在路網密度高時，擁塞度效能在大部分情況下是次糟。

對駕駛者而言，行車的舒適與否是考量的重點之一。因此當駕駛者開車時只考慮行車的舒適與否，地理+最新時戳法則的路況更新方法會是最佳的選擇。

4.4 小結

由上面所有的圖表得到的結果，將其條列式表示如下：

1. 針對網路中惡意訊息比例的分析

   i. 路網密度的變化對惡意訊息比例的影響不大。

   ii. 考慮惡意訊息回向的威脅車輛對網路的影響最大。

iii. 地理+加權時戳法則的路況更新方法可以有效的降低惡意封包的比例。

2. 針對車輛繞路比例和擁塞度的分析

i. 路網密度的變化會影響效能的變化。

ii. 對於繞路比例而言，加權時戳法則的路況更新方法效能最佳。

iii. 對於擁塞度而言，地理+最新時戳法則的路況更新方法效能最佳。

第五章 結論

5.1 結論

本研究結合了動態路徑導航模型以及 VANET 中的威脅模型和相關理論，提出了一個新的模型。在此模型中，會有威脅車輛的存在，威脅車輛為了自身的利益，而發送惡意訊息給其它車輛，而不是像過去動態路徑導航的研究一樣，只是為了讓駕駛者能有更好的行車路況。

表 5.1 效能優劣綜合整理

	繞路比例	擁塞度
最新時戳法則	4	4
加權時戳法則	1	3
地理+最新時戳	3	1
地理+加權時戳	2	2

經由模擬實驗，可以發現考慮惡意訊息回向的威脅車輛種類對網路的干擾最為嚴重；而地理+加權時戳法則的路況更新方法最能抵抗惡意訊息的干擾。在效能的分析上，如表 5.1 所示。考慮繞路比例，加權時戳法則的路況更新方法效能最好；考慮擁塞度，地理+最新時戳法則的路況更新方法效能最好。而最新時戳

法則的路況更新方法效能都是最差的。整體而言，雖然地理+加權時戳法則的路況更新方法都不是最佳的，但平均來說效能會是最佳的。

在車間通訊的偽造訊息攻擊難以偵測。威脅車輛為了私益傳送偽造路況資訊給其它車輛，在當下其它車輛無法立即查覺，即使事後知道某些路段是順暢的，但無法確定這些路段是否一直保持順暢的狀態，而不是從擁塞的狀態變成順暢的狀態，因此在車間通訊的偽造訊息攻擊，在當下和事後接難以驗證。其中一種可行的方案是混合車間通訊和車路通訊的環境則可以執行偵測的行動。透過車輛經過路側裝置的時間以及訊號的強弱可以推算車輛的行駛路徑以及時間，控管中心藉由推算出的車輛行駛路徑和時間，和訊息封包的路況資訊表做比對，如果路段的旅行時間和時戳值落差很大，表示車輛即為威脅車輛。在這種分散式且車輛不用做上線認證的環境中，建議使用黑名單的處罰方式，亦即當控管中心發現威脅車輛後，及登錄此車輛之 ID 進入黑名單，再藉由路側裝置發送給路上之車輛，當車輛發現黑名單的車輛時，則不使用其訊息封包，也不發送訊息封包給黑名單內之車輛，以達到處罰的效果。

對駕駛者而言，開車一般都會考慮是否省油或是行車舒適與否。本論文透過模擬，建議強調省油的駕駛人使用加權時戳法則的路況更新方法；建議強調舒適的駕駛人使用地理+最新時戳法則的路況更新方法。而沒有特別偏好的駕駛者，建議使用地理+加權時戳法則的路況更新方法。

對汽車導航業者來說，路上出現威脅車輛，而此時會希望自己的產品能夠在具有威脅的環境下有效的抵抗惡意訊息的干擾，並且效能還能保持一定的水準。本研究透過模擬，建議汽車導航業者在路況更新的方法上，可以使用地理+加權時戳法則的路況更新方法。

5.2 未來展望

在混合車間通訊和車路通訊的環境中，控管中心或是負責做驗證的單位可以有效偵查進行偽造訊息攻擊的車輛。可是在純車間通訊的環境中，尚無法針對偽造訊息攻擊做出有效的偵測。未來動態導航系統如果朝純車間通訊的環境發展並且推出使用，則偽造訊息攻擊將會是一個最大的問題。

由於本研究的重點放在威脅車輛的相關容忍度研究上，為了避免失焦，所以在路網以及車輛的設定上加以簡化，在本模型的基礎特性釐清後，將來可以加入以使模型更加真實，以下列舉之：

1、 路網的設置：

A. 單線雙向道：在本研究中，道路皆為單線雙向道，可是真實路網中，如果不是重劃過的都市，依據是否為市區或是道路的特性，常常是雙線以上的雙向道亦或是單向道，而且會在路網中錯縱複雜的交錯著。

B. 道路不限速：本研究為了簡化，因此不對道路作限速的動作。可是真實路網會依據路段的特性，做出限速的動作。

2、 車輛移動模式：

A. 駕駛者統一化：每個人的個性都是不一樣的，所以開車的習慣都會不一樣。可能有些人喜歡開慢車；有些人則喜歡開快車。或如安全車距的拿捏，每個人也都不同。踩油門以及最感到舒適的車速也都不一樣。

B. 車速變更模式：本研究為了簡化，所以加速度皆設定為 1，最高速度和最低速度也有所設定。可是依據車輛的品牌和性能的不同，每臺車的加速度和最高速度也會不同。

C. 車輛皆為小客車：避免複雜，本研究車輛皆設定為小客車。真實路網除了小客車外，還有大大小小不同的其它車輛存在。除了汽車之外，真實路網還會有摩托車、腳踏車等等交通工具的存在。

參考文獻

Abolhasan, M., Wysocki, T., & Dutkiewicz, E. (2004). A review of routing protocols for mobile ad hoc networks. *Ad Hoc Networks , 2*, pp. 1-22.

Bechler, M., & Wolf, L. (2005). Mobility management for vehicular ad hoc networks. *Vehicular Technology Conference*, (pp. 2294-2298).

Bernsen, J., & Manivannan, D. (2009). Unicast routing protocols for vehicular ad hoc networks: A critical comparison and classification. *Pervasive and Mobile Computing , 5*, pp. 1-18.

Biswas, S., Tatchikou, R., & Dion, F. (2006, January). Vehicle-to-Vehicle Wireless Communication Protocols for Enhancing Highway Traffic Safety. *IEEE Communications Magazine* , 74-82.

Blum, J. J., Eskandarian, A., & Hoffman, L. J. (2004). Challenges of Intervehicle Ad Hoc Networks. *IEEE Transaction on Intelligent Transportation Systems , 5* (4), pp. 347-351.

Boone, C., Brabander, B. D., & Witteloostuijn, A. V. (1999). The impact of personality on behavior in five Prisoner's Dilemma games. *Journal of Economic Psychology , 20*, pp. 343-377.

Chang, B. R., Tsai, H. F., & Young, C. P. (2010). Intelligent data fusion system for predicting vehicle collision warning using vision/GPS sensing. *Expert Systems with Applications , 37* (3), pp. 2439-2450.

Costa, P., Frey, D., Migliavacca, M., & Mottola, L. (2006). Towards Lightweight Information Dissemination in Inter-Vehicular Networks. *3rd international workshop on Vehicular ad hoc networks*, (pp. 20-29).

Douceur, J. R. (2002). *The Sybil Attack.* 1st International Workshop on Peer-to-Peer Systems (IPTPS '02), Cambridge, MA.

Garg, A., & Reddy, A. N. (2004). Mitigation of DoS attacks through QoS regulation. *Microprocessors and Microsystems , 28*, pp. 521-530.

Karp, B., & Kung, H. (2000). GPSR: greedy perimeter stateless routing for wireless sensor networks. *6th Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom '00).*

Kitani, T., Shinkawa, T., Shibata, N., Yasumoto, K., Ito, M., & Higashino, T. (2008). Efficient VANET-Based Traffic Information Sharing using Buses on Regular Routes. *Vehicular Technology Conference.*

Kofman, F., & Lawarree, J. (1996). A prisoner's dilemma model of collusion deterrence. *Journal of Public Economics , 59*, pp. 117-136.

Korkmaz, G., Ekici, E., Ozguner, F., & Ozguner, U. (2004). Urban Multi-Hop BroadcastProtocol for Inter-Vehicle Communication Systems. *1st ACM international workshop on Vehicular ad hoc networks*, (pp. 1-10).

Legge, S. (1996). Cooperative lions escape the Prisoner's Dilemma. *Trends in Ecology & Evolution , 11*, pp. 2-3.

Leinmuller, T., Schoch, E., & Kargl, F. (2006). Position verification approaches for vehicular ad hoc networks. *IEEE Wireless Communications* , pp. 16-21.

Leinmuller, T., Schoch, E., Kargl, F., & Maihofer, C. (2005). Influence of Falsified Position Data on Geographic Ad-Hoc Routing. *second European Workshop on Security and Privacy in Ad hoc and Sensor Networks.*

Li, L., Rus, D., & Haas, Z. (2002). Gossip-based ad hoc routing. *Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies*, *3*, pp. 1707- 1716.

Lin, X., Sun, X., & Shen, X. (2007). GSIS: A Secure and Privacy-Preserving Protocol for Vehicular Communications. *IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY , 56* (6), pp. 3442-3456.

Little, T. D., & Agarwal, A. (2005). An information propagation scheme for VANETs. *Intelligent Transportation Systems*, (pp. 13-15).

Liu, C., & Yu, J. T. (2006). An analysis of DoS attacks on wireless LAN. *6th IASTED Int. Multi-Conf. Wireless Opt. Commun.*, (pp. 346–351). Banff, AB, Canada.

Marco, F., Jerome, H., Fethi, F., & Christian, B. (2007). Vehicular Mobility Simulation for VANETs. *40th Annual Simulation Symposium*, (pp. 301-309).

Ohara, K., Nojima, Y., & Ishibuchi, H. (2007). A Study on Traffic Information Sharing Through Inter-Vehicle Communication. *22nd IEEE International Symposium on Intelligent Control Part of IEEE Multi-conference on Systems and Control*, (pp. 670-675). Singapore.

Poundstone, W. (1992). *Prisoner's Dilemma.* New York: Oxford University Press.

Rabow, G. (1988). The social implications of nonzero-sum games. *IEEE Technology and Society Magazine , 7*, 12-18.

Surbey, M. K., & McNally, J. J. (1997). Self-deception as a mediator of cooperation and defection in varying social contexts described in the iterated prisoner's dilemma. *Evolution and Human Behavior , 18*, pp. 417-435.

Taleb, T., Ochi, M., Jamalipour, A., Nei, K., & Nemoto, Y. (2006). An efficientvehicle-heading based routing protocol for VANET networks. *IEEE Wireless Communications and Networking Conference (WCNC 2006).*

Tang, A., & Yip, A. (2010). Collision avoidance timing analysis of DSRC-based vehicles. *Accident Analysis and Prevention , 42*, pp. 182-195.

Toh, C. K. (2002). *Ad Hoc Mobile Wireless Networks. Protocols and Systems.* New Jersey: Prentice Hall PTR.

Uno, K., & Namatame, A. (1999). Agent-based simulation for policy issue. *IEEE International Conference on Systems, Man, and Cybernetics.*

Yan, G., Olariu, S., & Weigle, M. C. (2008). Providing VANET security through active position detection. *Computer Communications , 31*, pp. 2883-2897.

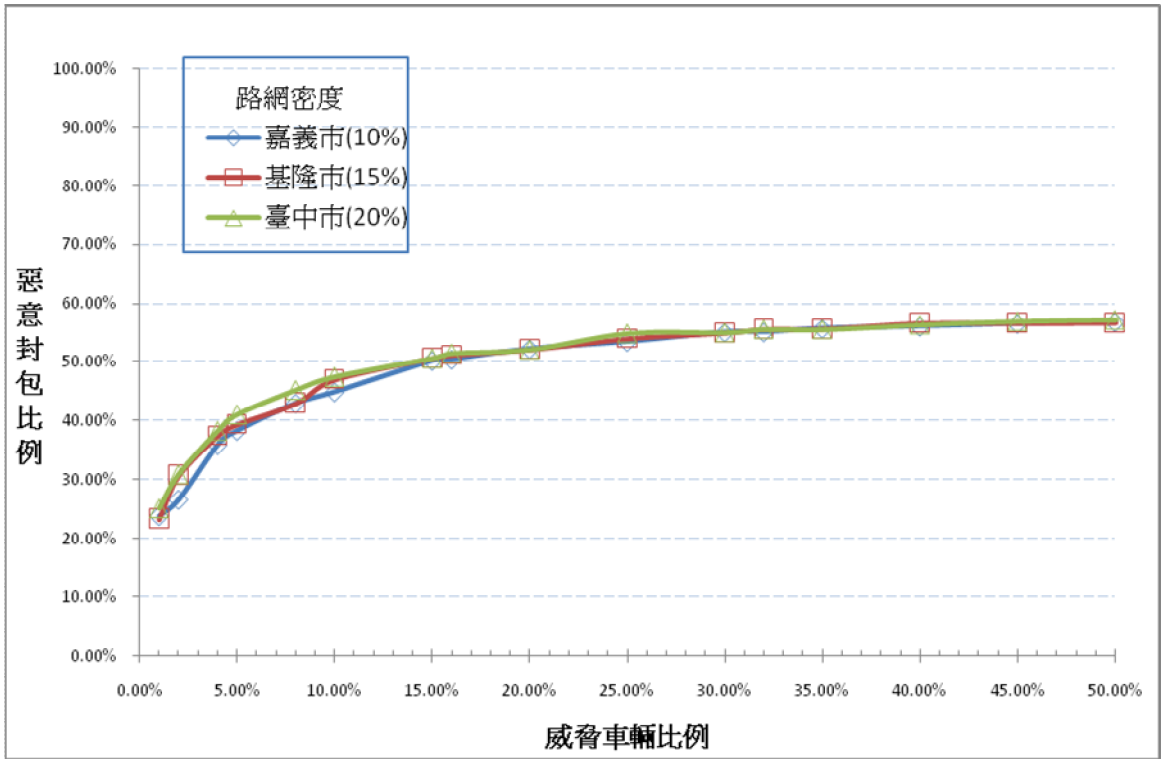
Yanlin, P., Abichar, Z., & Chang, J. M. (2006). Roadside-Aided Routing (RAR) in Vehicular Networks. *Communications, IEEE International conference*, *8*, pp.

3602-3607.

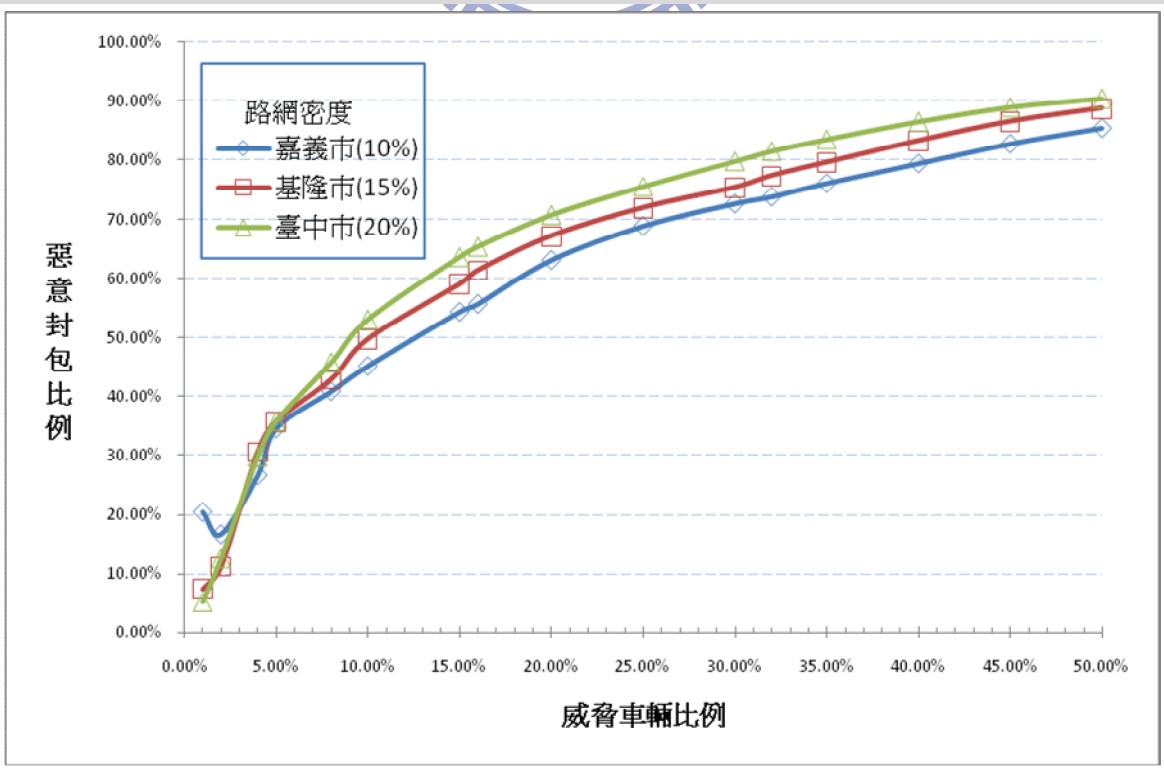
Zhao, J., & Cao, G. (2008). VADD：Vehicle-Assisted Data Delivery in Vehicular Ad Hoc Networks. *IEEE Transactions on Vehicular Technology , 57* (3), pp. 1910-1922.

附錄 A

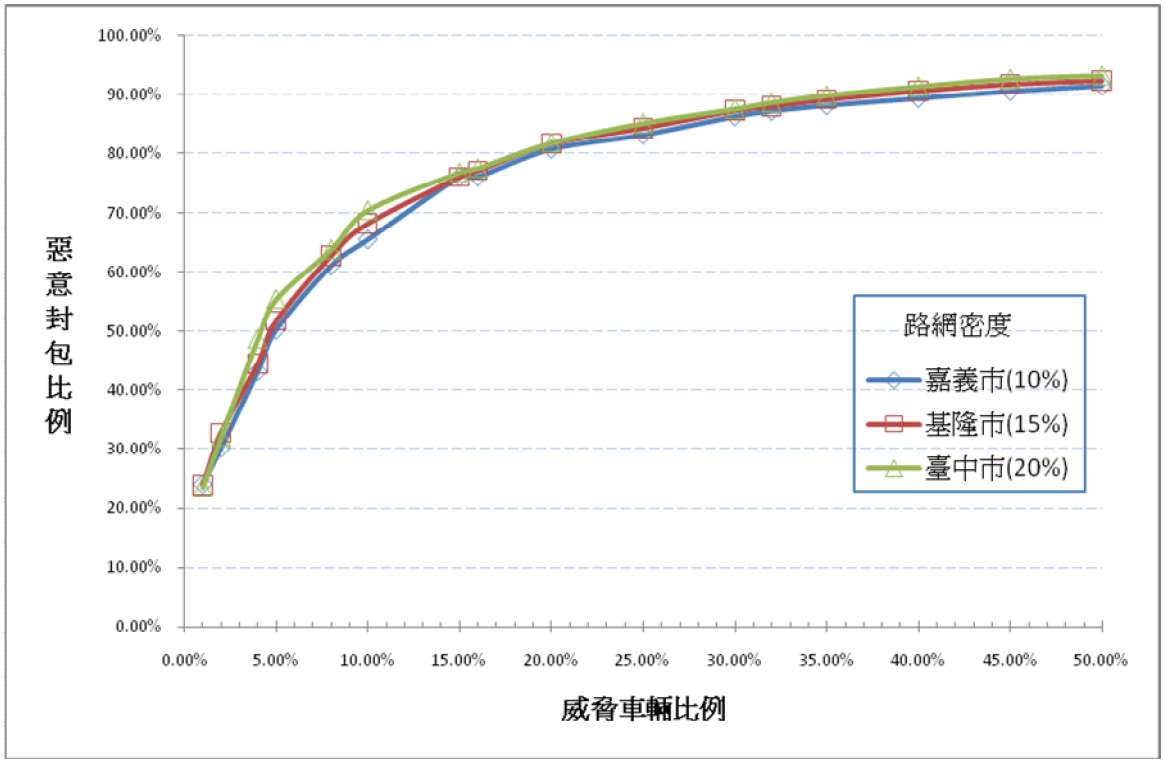
(a)最新時戳法則



(b)加權時戳法則



(c)地理+最新時戳法則



(d)地理+加權時戳法則

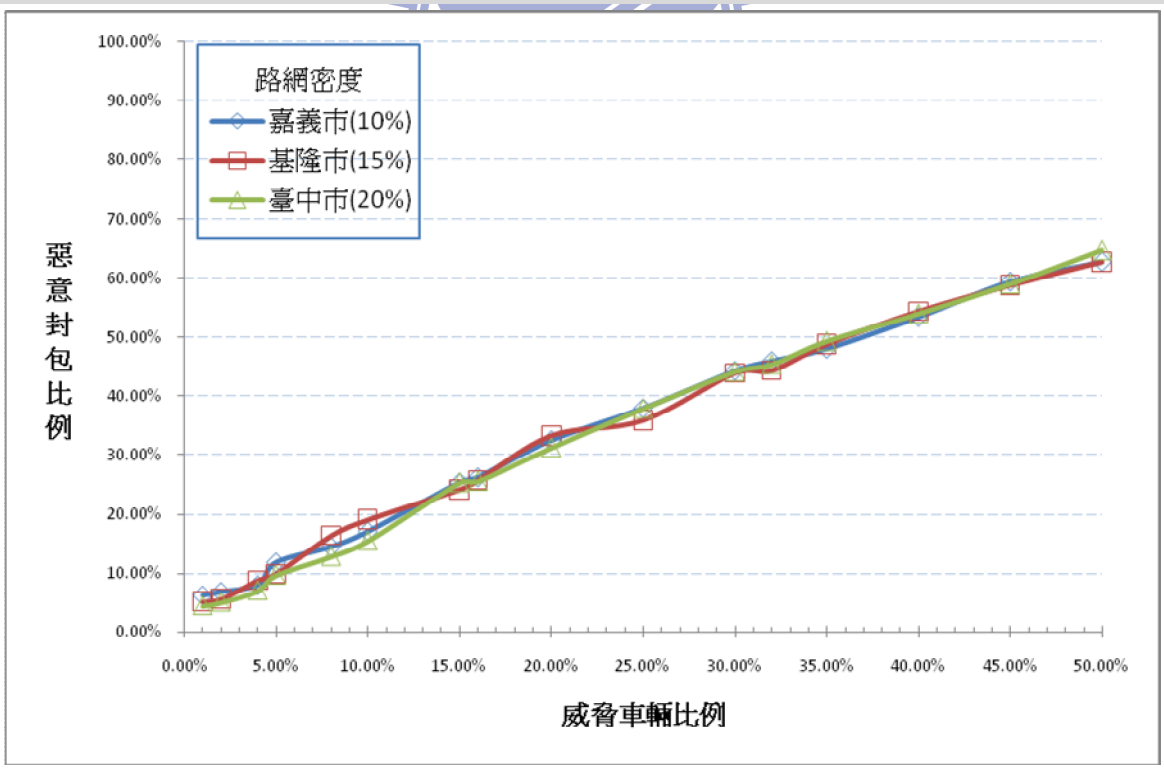
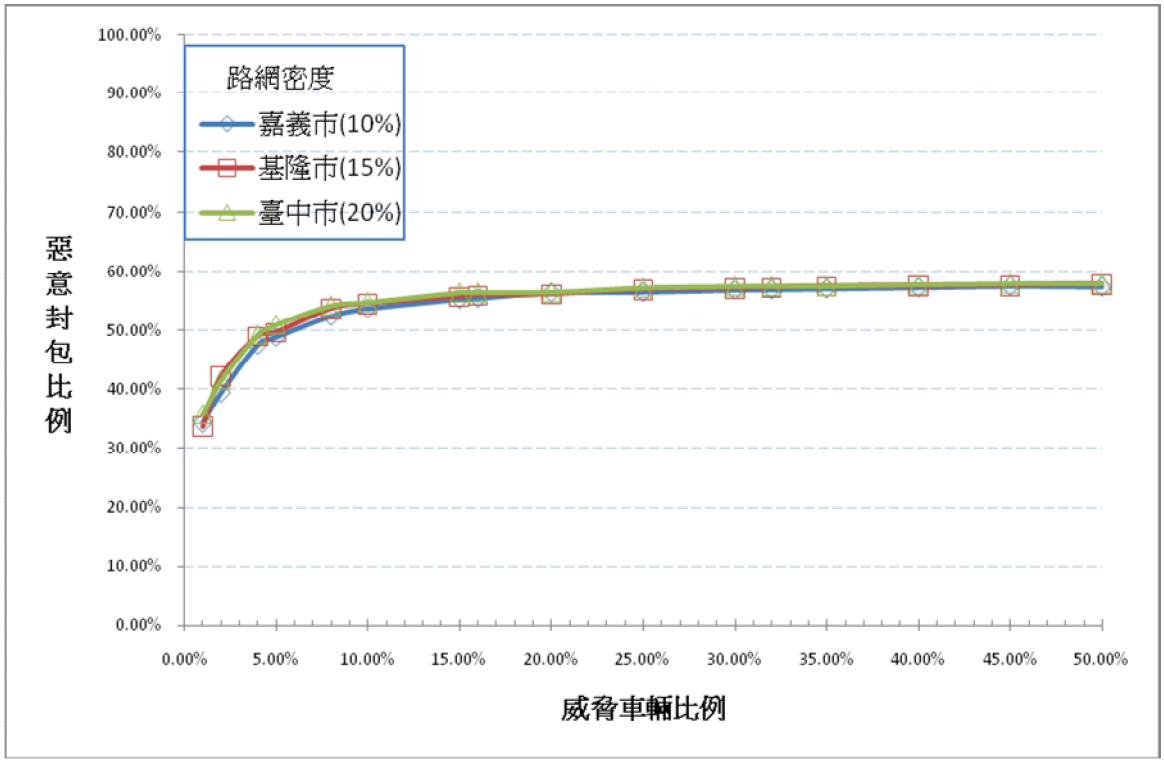
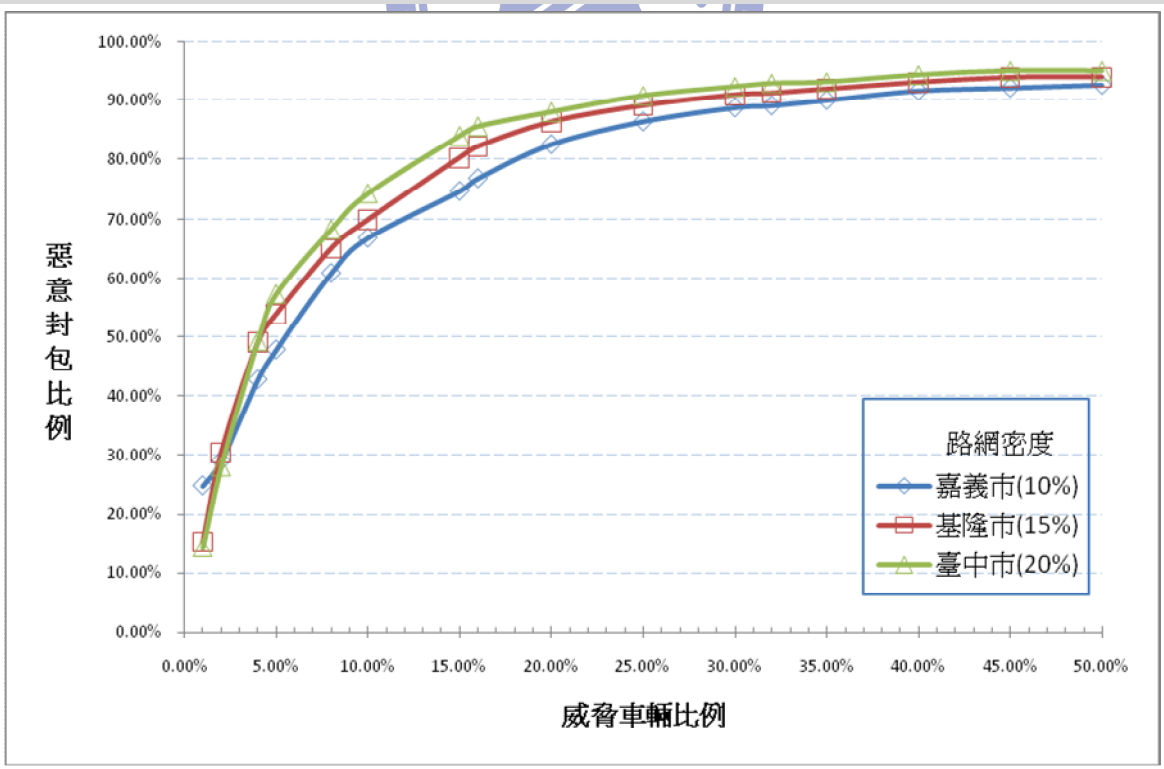


圖 A.1 偽造路況：路網密度對網路影響之分析

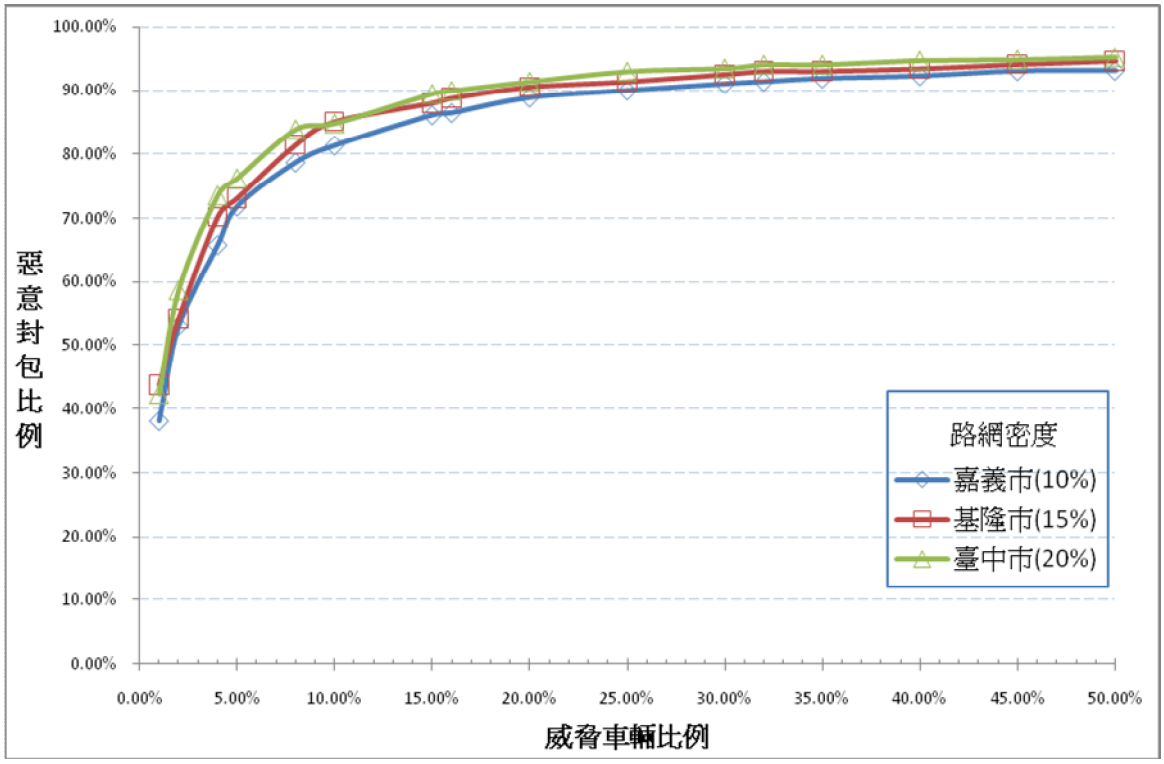
(a)最新時戳法則



(b)加權時戳法則



(c)地理+最新時戳法則



(d)地理+加權時戳法則

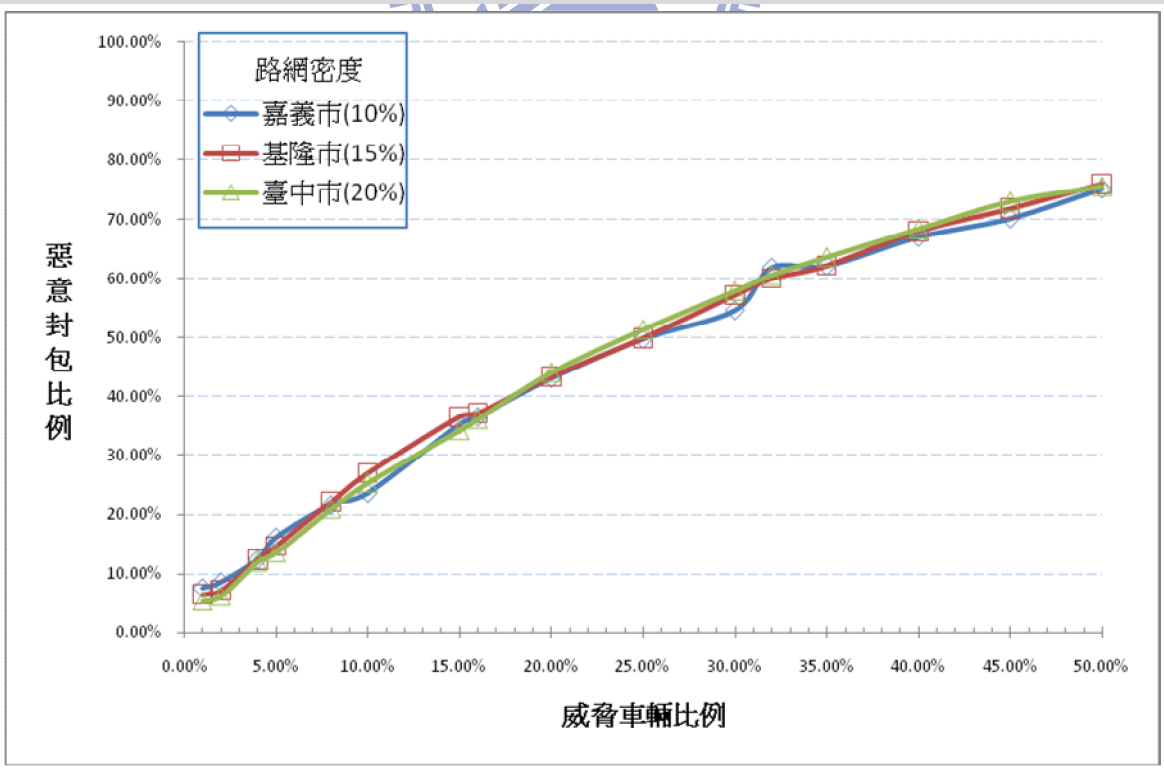
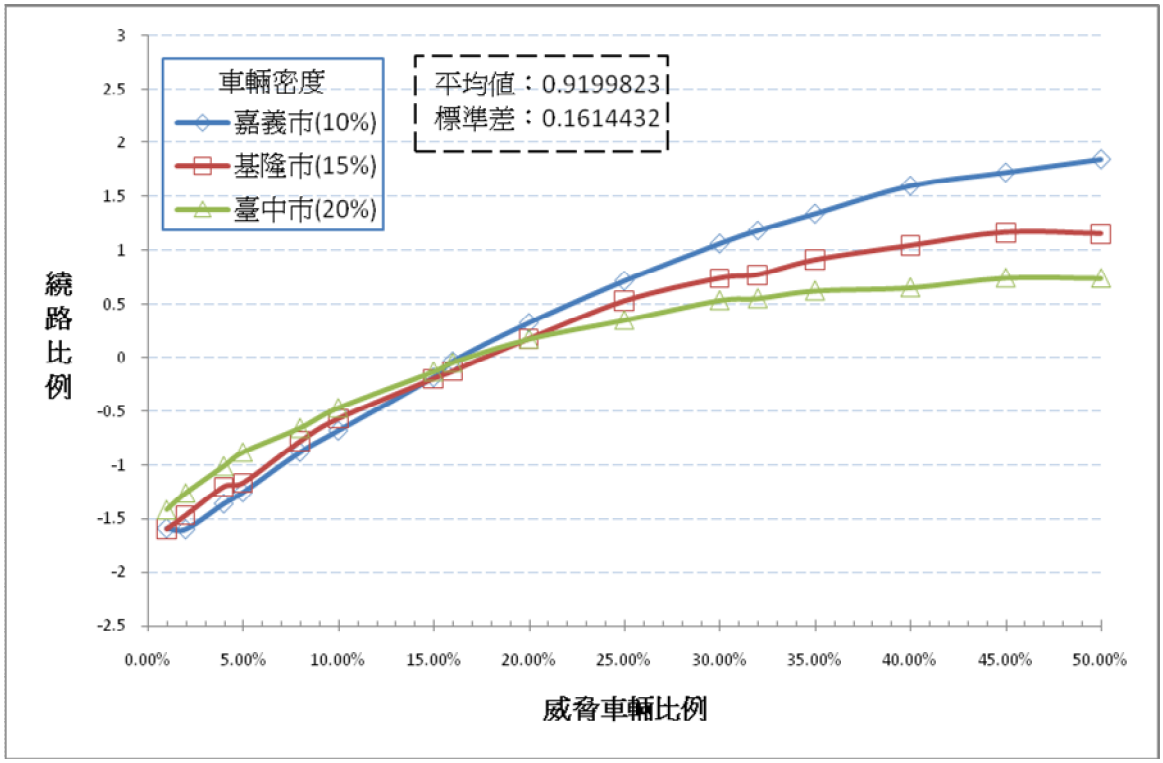


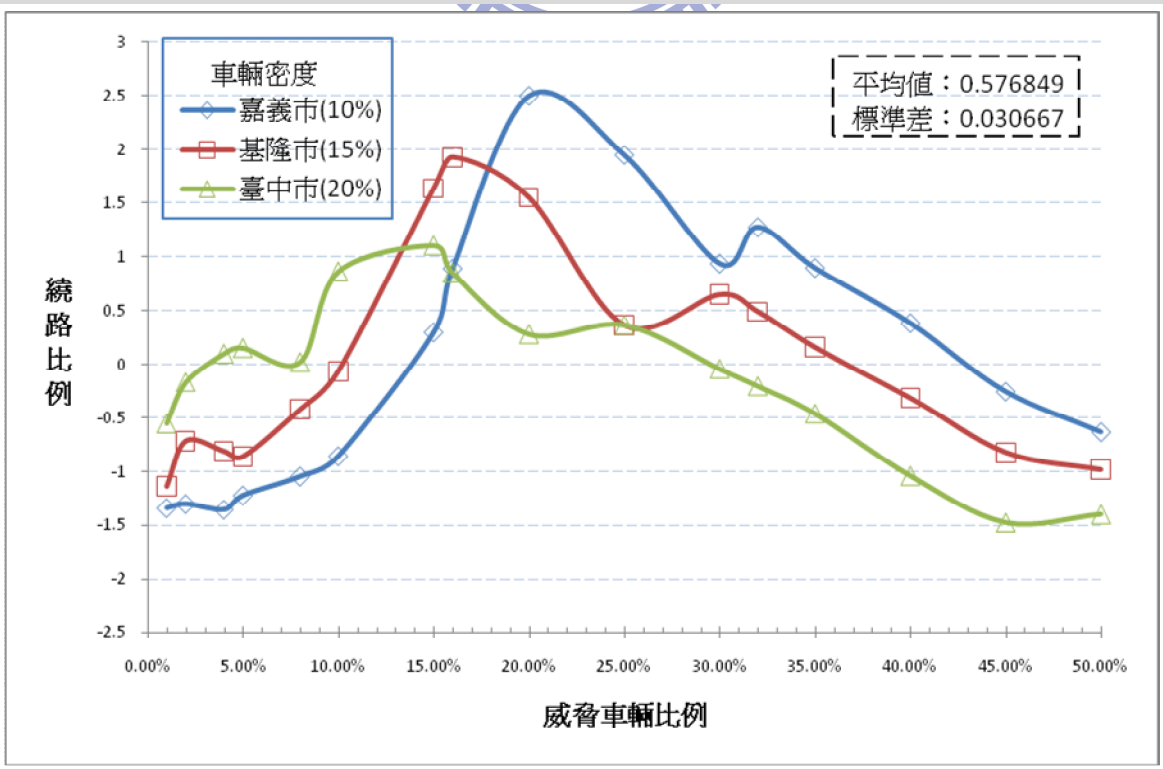
圖 A.2 偽造路況和時戳：路網密度對網路影響之分析

附錄 B

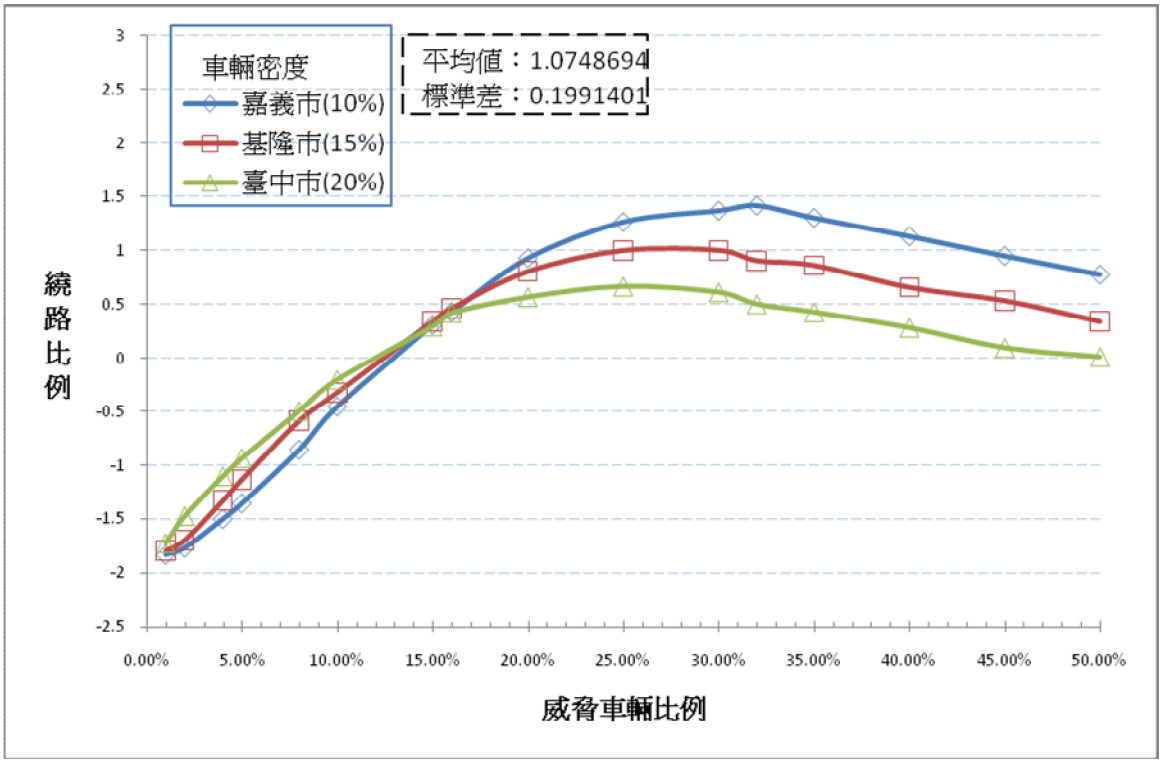
(a)最新時戳法則



(b)加權時戳法則



(c)地理+最新時戳法則



(d)地理+加權時戳法則

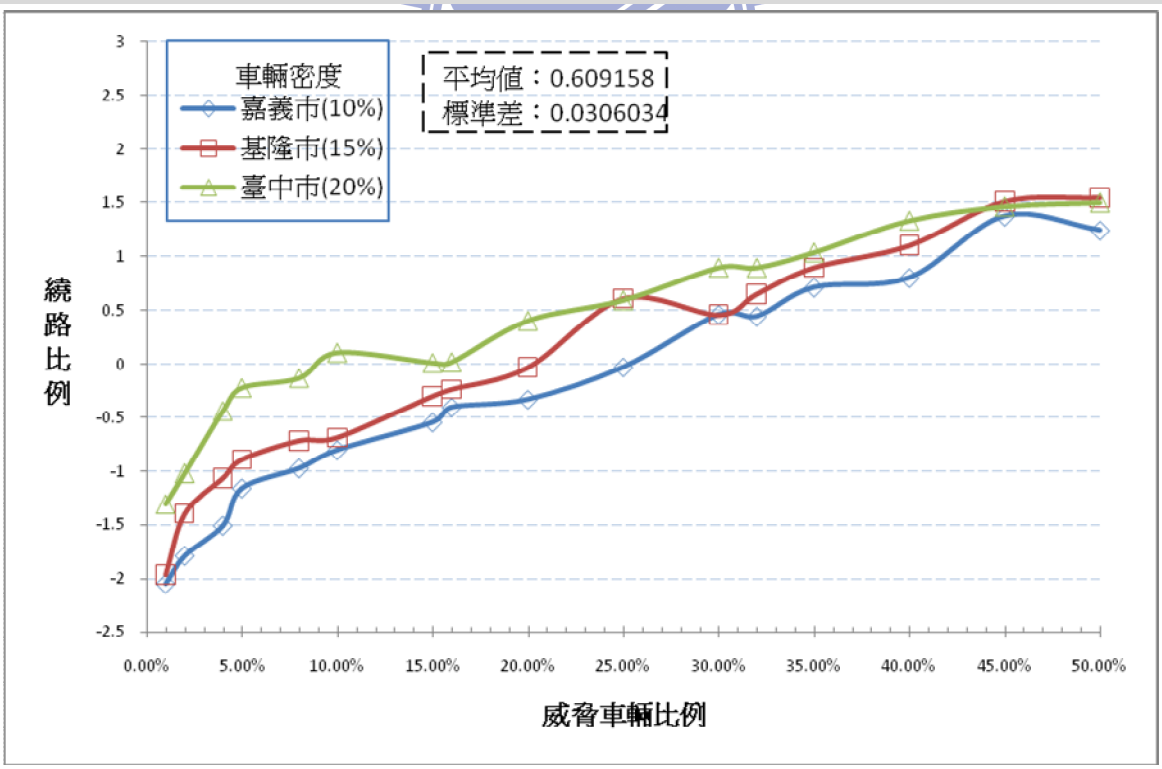
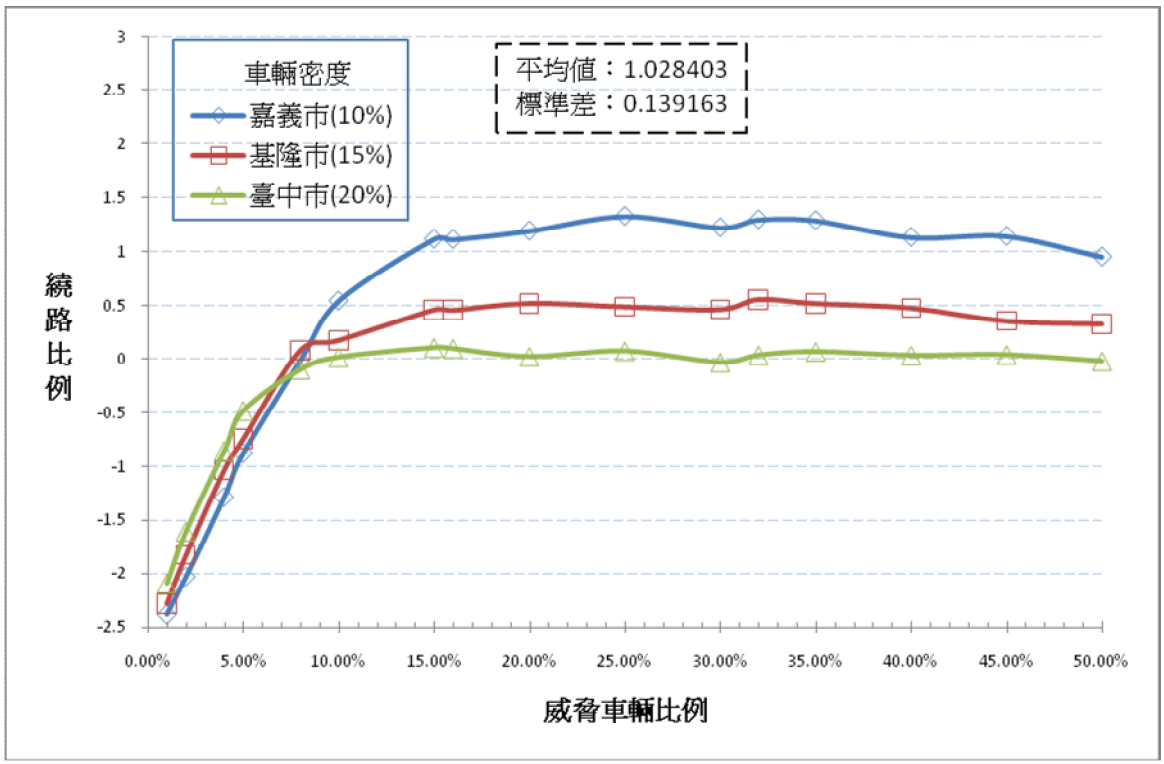
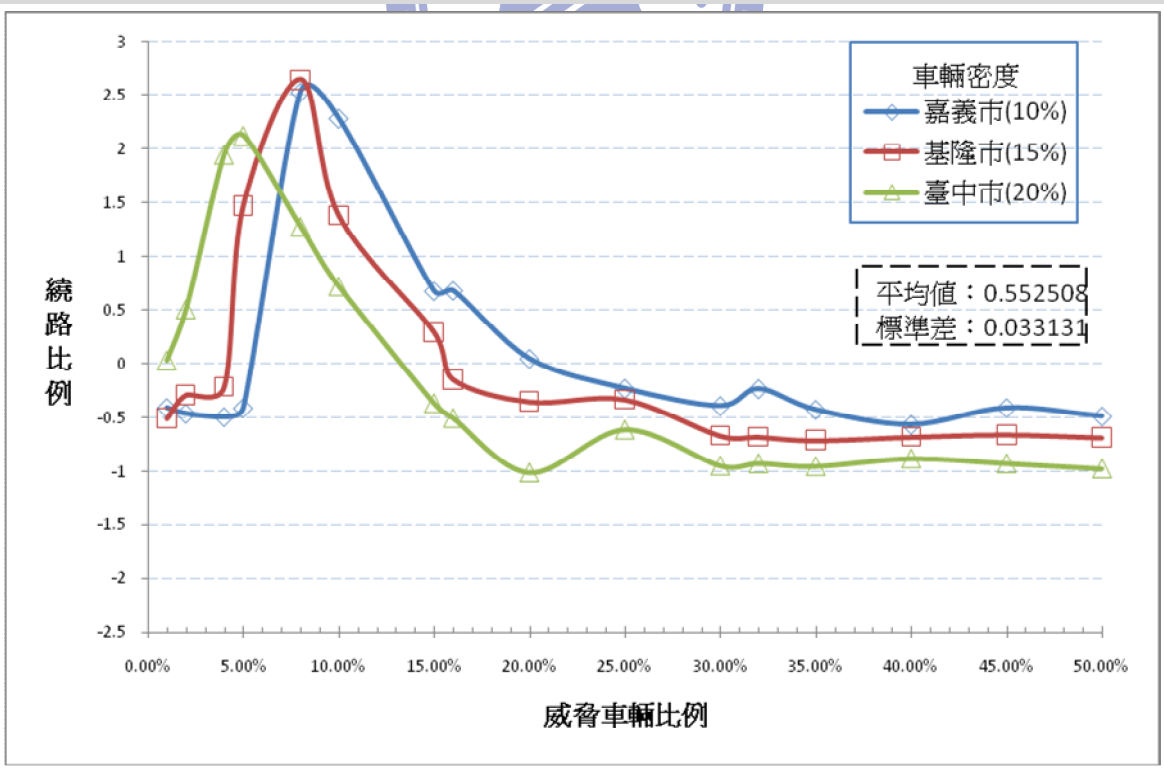


圖 B.1 偽造路況：路網密度對繞路比例影響之分析

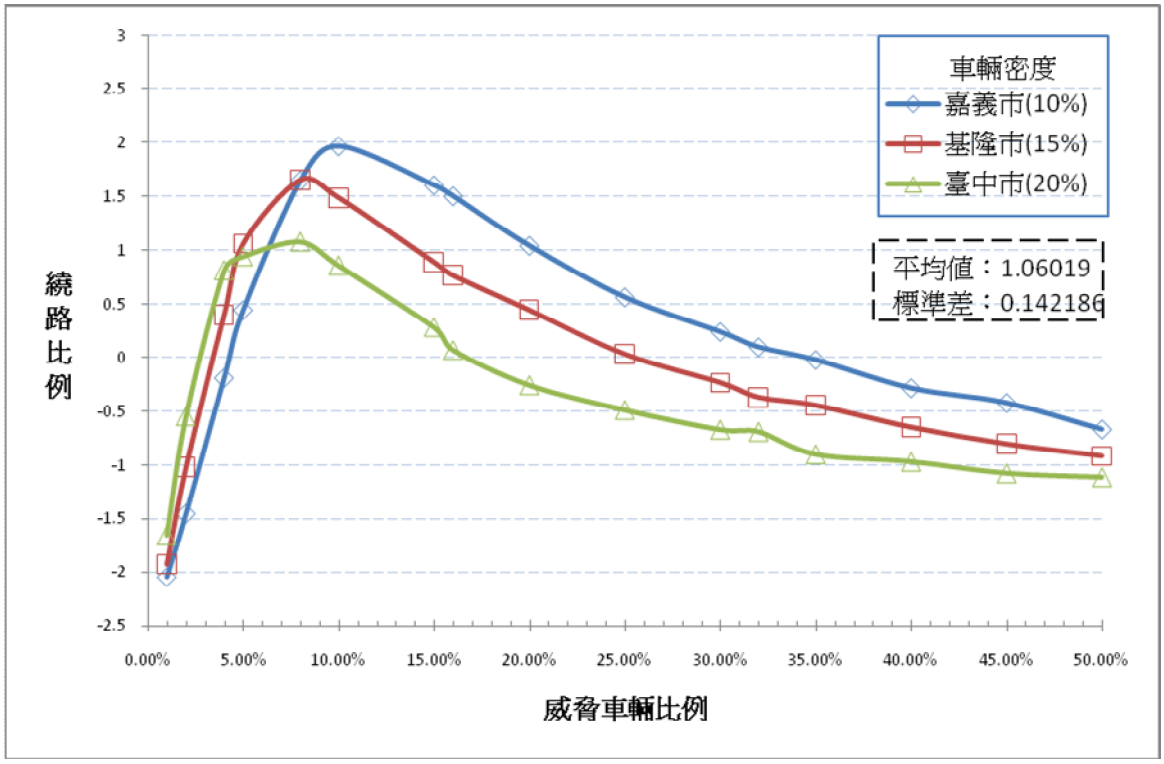
(a)最新時戳法則



(b)加權時戳法則



(c)地理+最新時戳法則



(d)地理+加權時戳法則

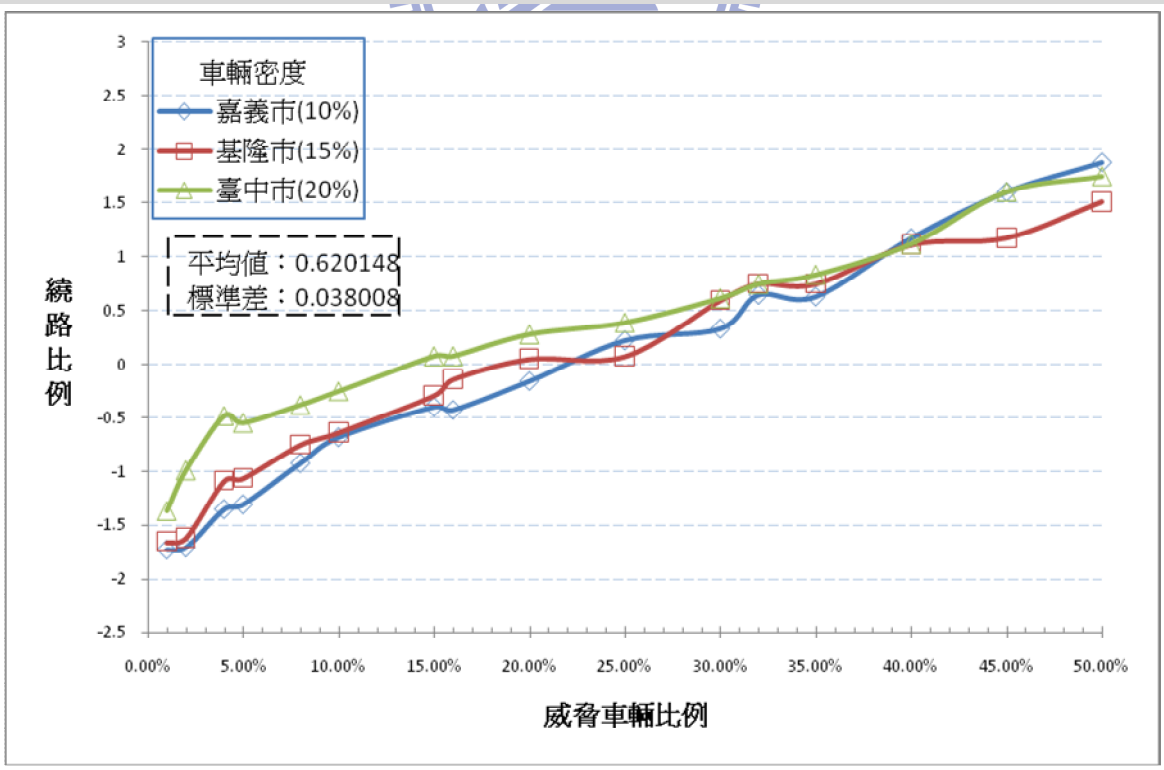
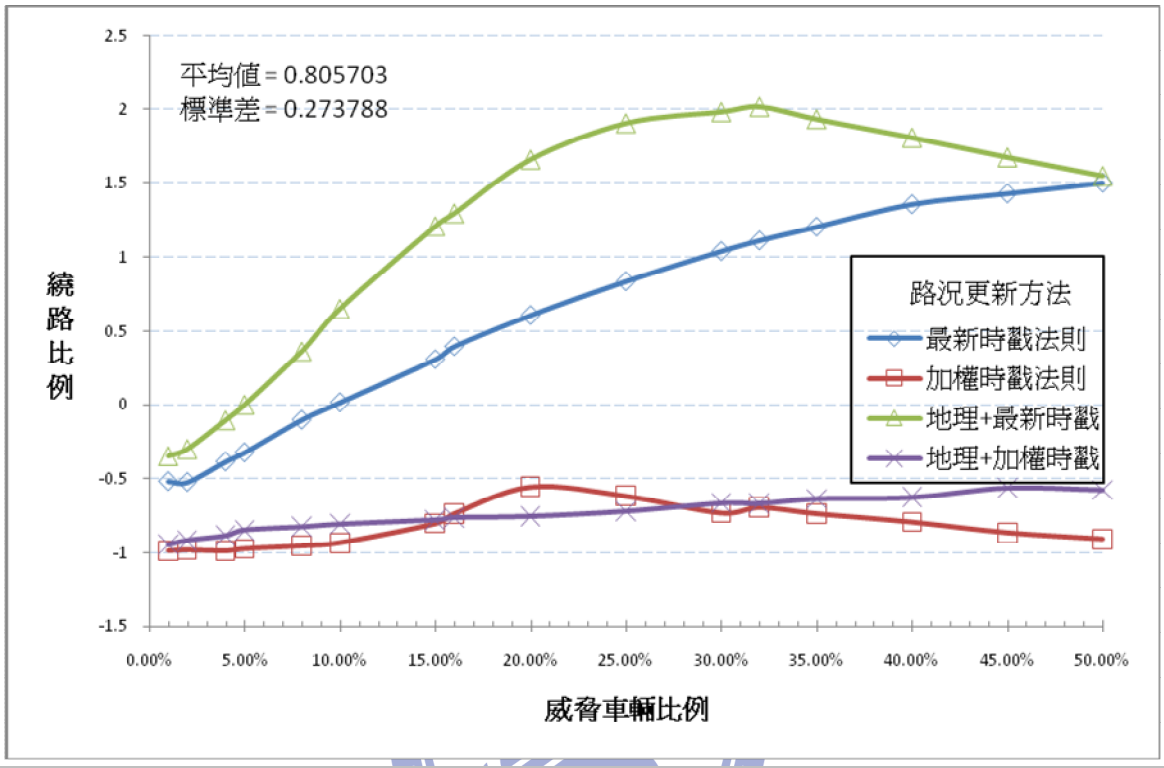


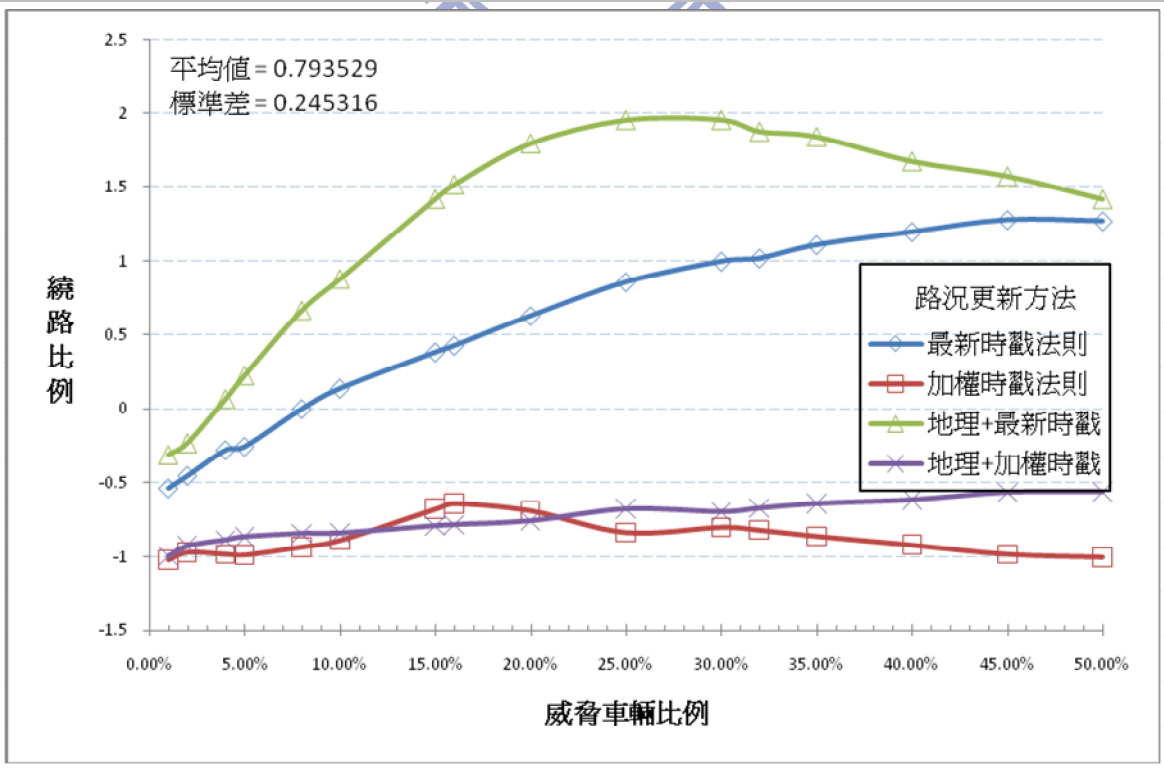
圖 B.2 偽造路況和時戳：路網密度對繞路比例影響之分析

附錄 C

(a)嘉義市(10%)



(b)基隆市(15%)



(c)臺中市(20%)

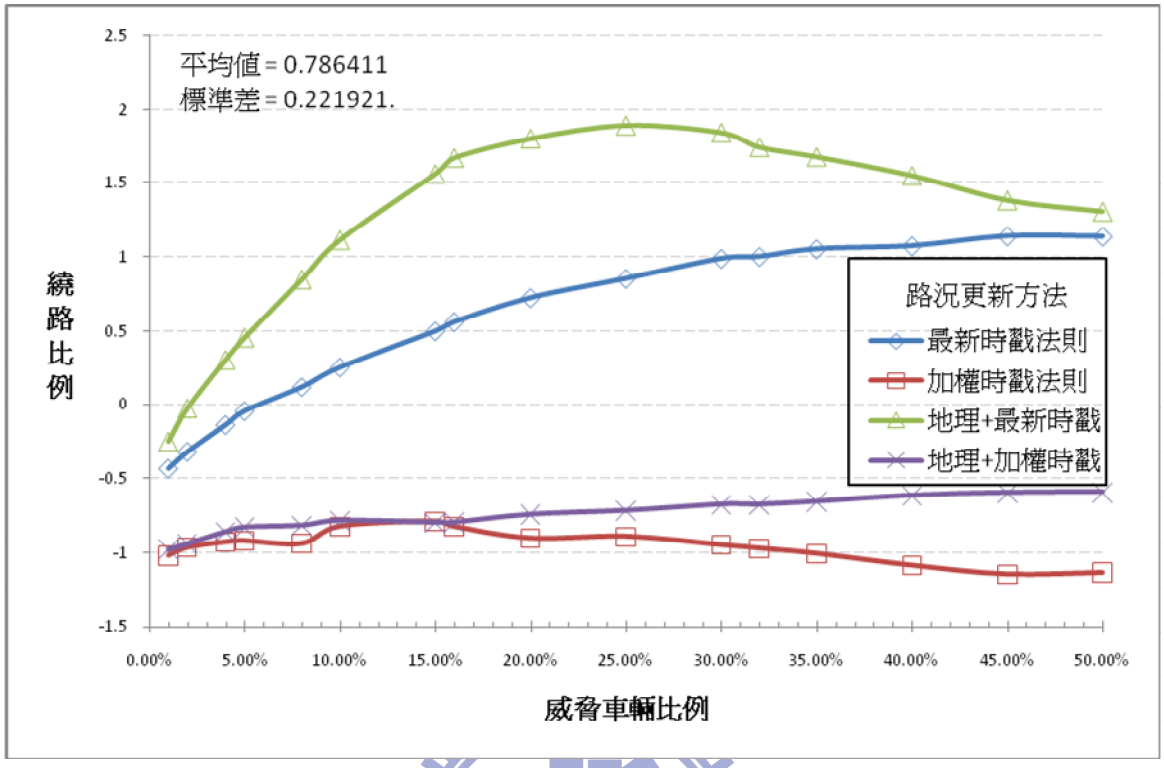
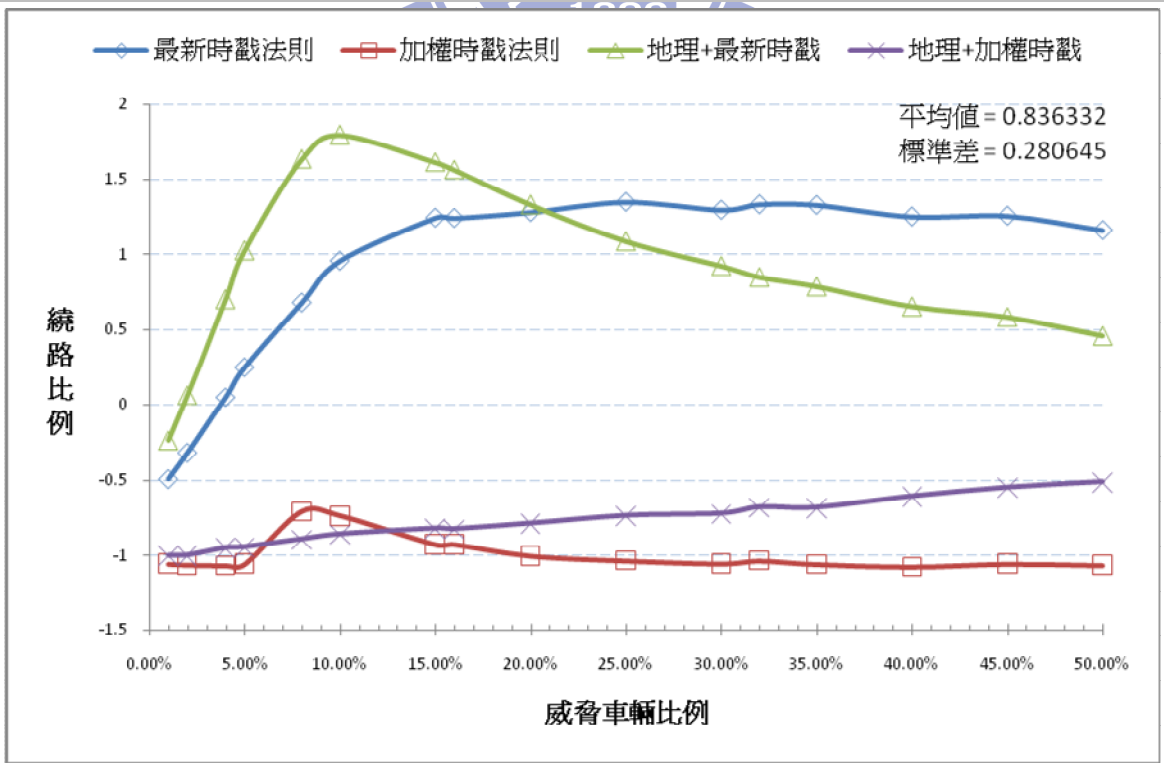
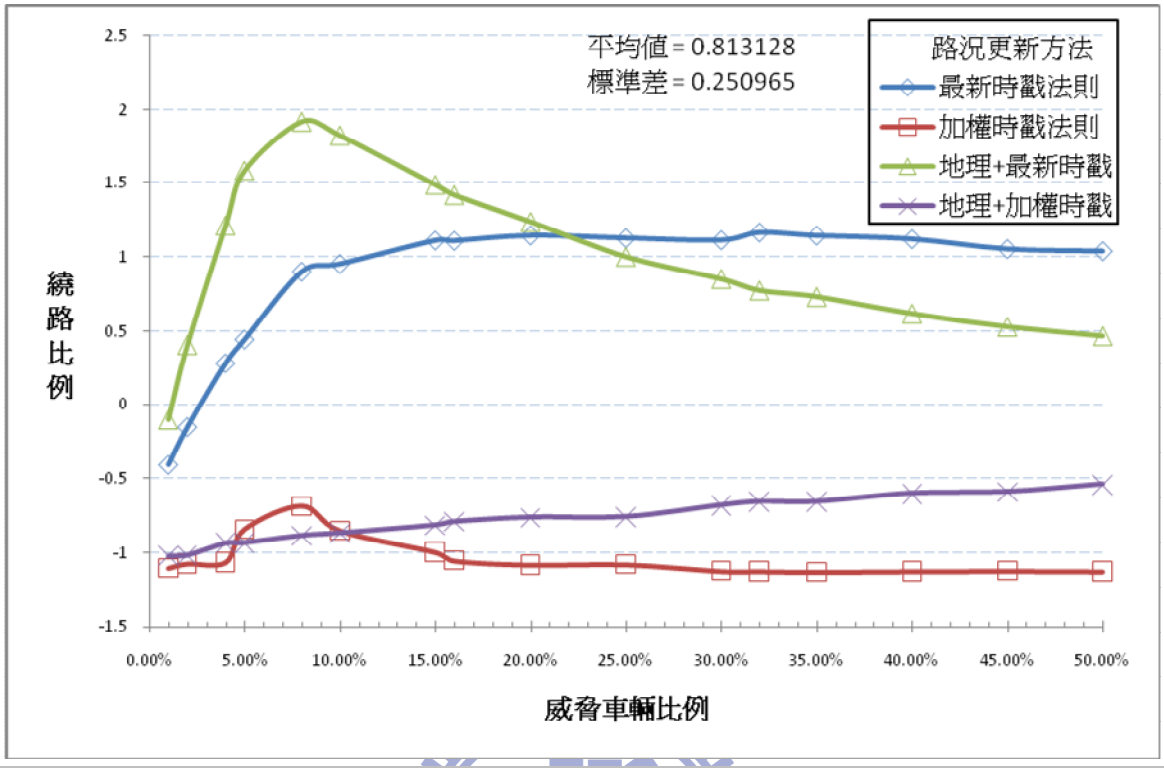


圖 C.1 偽造路況：路況更新方法對繞路比例影響之分析

(a)嘉義市(10%)



(b)基隆市(15%)



(c)臺中市(20%)

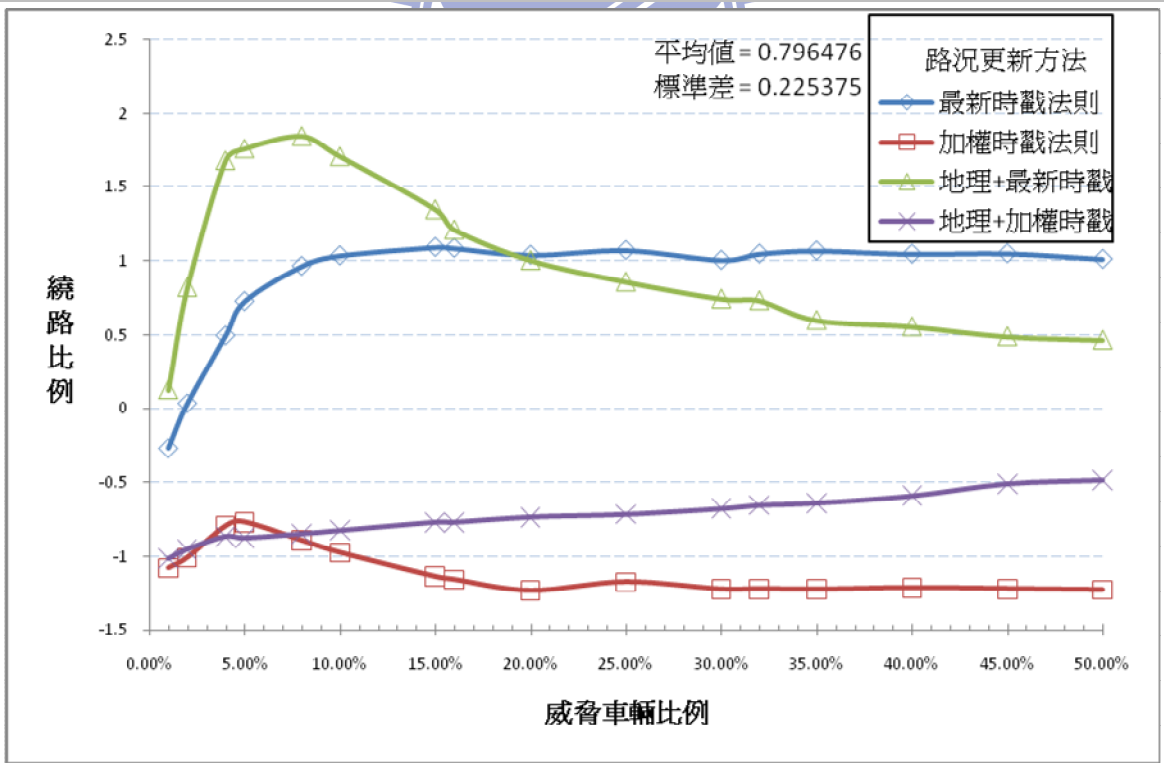


圖 C.2 偽造路況和時戳：路況更新方法對繞路比例影響之分析