國立交通大學

資訊管理研究所

碩士論文

一個針對行動無基礎網路中的信任證據產生、散佈與信任值計算機制

A Trust Evidence Establishment, Distribution and Value Computation Mechanism for Mobile Ad Hoc Networks

研究生：黃展翊

指導教授：羅濟群 博士

中華民國　　九十六年　　六月

一個針對行動無基礎網路中的信任證據產生、散佈與信任值計算機制

A Trust Evidence Establishment, Distribution and Value Computation Mechanism for Mobile Ad Hoc Networks

研 究 生：黃展翊　　Student: Chan-Yi Huang

指導教授：羅濟群　　Advisor: Chi-Chun Lo

國立交通大學

資訊管理研究所

碩士論文

A Thesis

Submitted to Institute of Information Management

College of Management

National Chiao Tung University

in Partial Fulfillment of the Requirements

for the Degree of

Master of Science

in

Information Management

June 2007

Hsinchu, Taiwan, the Republic of China

中華民國　　九十六 年　六 月

一個針對行動無基礎網路中的信任證據產生、散佈與信任值計算機制

研究生：黃展翊　　指導教授：羅濟群 博士

國立交通大學

資訊管理研究所

摘要

身分認證在行動無基礎網路中是網路使用者識別的基礎方式，讓周圍節點確認往後將要通訊的對象。又為了衡量通訊節點的行為，可將節點識別和信任程度相互結合，以達到資料轉送的安全。然而在行動無基礎網路中的節點為互相獨立且為完全自我組成架構，所以必須擬定一套包含身分識別、憑證資訊、以及信任機制的整體信任證據運作，並在線上做信任證據產生、散佈、衡量、以及驗證。

本研究針對行動無基礎網路提出一個分散式的信任證據運作機制，讓網路節點可以各自產生代表己方的憑證並擁有相關的信任識別，而不用中央管理端控管，以作為節點的識別、傳送、衡量。信任證據管理方法可讓信任證據在網路中經由傳送來得到節點的資訊，且不會被假造或修改。節點在經過互動後，信任值高的節點可透過信任值重新衡量適時反應先前階段的互動結果。於實驗中證明此信任證據運作方式可以解決自私節點和惡意節點的問題，並可以在行動無基礎網路中得到最好的路由參考。運用賽局理論也可證明節點合作可以得到最大的利益，若中繼節點採取背離的策略，則此節點會因為信任值的降低而成為不受信任的節點，故傳送資料時也會遭受其他節點的拒絕，直到合作為止。

關鍵字：行動無基礎網路、信任證據、信任產生、信任散佈、信任成員、信任節點、信任值、總信任值、賽局理論

A Trust Evidence Establishment, Distribution and Value Computation Mechanism for Mobile Ad Hoc Networks

Student: Chan-Yi Huang Advisor: Dr. Chi-Chun Lo

National Chiao Tung University

Institute of Information Management

Abstract

Personal identity is the basic way to present user's role for MANETs, so all around nodes can verify the node which they will communicate with in the future. In order to evaluate the node's behavior, we can combine the identity with trust value. But nodes are in independent and self-configured architecture, so it is important to develop a totally trust evidence which contains personal identity, certificate information, and trust operation mechanism. Moreover, the trust evidence can be established, distributed, evaluated, and verified on-line.

This research proposes the distributed trust evidence operation mechanism for MANETs. The node establishes certificate itself and has corresponding trust identity without central certificate authority. The way to manage trust evidence can get others' trust evidence via the transmission of packets and would not be modified by malicious nodes. The model will resolve selfish node and malicious node problem via simulation. It will be suitable to operate MANETs and provide most correct routing reference. We can also prove that nodes in MANETs will cooperate via game theory. After interaction, higher trust nodes can reflect the outcome and re-evaluate the trust. If the intermediate node deviates, its trust value will be decreased and will be regarded as the doubtful node. Therefore when the doubtful node requests surrounding node to forward packets, it will be rejected until the node cooperates.

Key words: mobile ad hoc networks, trust evidence, trust establishment, trust distribution, trust member, trust node, trust value, total trust value, game theory

誌謝

本論文的完成首先感謝家人對我的支持與鼓勵，當我遇到困難時雖然他們無法提供技術上的支持，但是在精神上的鼓勵使得我能不畏失敗繼續挑戰。

感謝羅濟群老師在研究上給我的指導及指教，雖然我有時呈現的進度無法令老師滿意，但是老師不厭其煩的修正且可耐心的解答我的問題，我會遵照老師的教誨並在往後工作及處世中追求最好的表現。

其次感謝實驗室的俊傑、鼎元、智超以及友義學長對我論文的建議及改正，在我低潮的時候安慰我，並適時的在論文的每一個階段提示正確的方向。還有實驗室的學長姐、同學和學弟，有你們的地方充滿著歡笑，讓我的研究過程不會感到枯燥乏味，反之實驗室的氣氛使得我能以輕鬆的態度迎接挑戰。同時感謝聖鈞和崴逸同學的鼓勵，使得我在遇到瓶頸的時候能給我多方面的建議。

最後感謝去年過世的外婆，雖然無法在您面前畢業，但是我答應您會好好的認真讀書及工作，希望您在天之靈可以感受到我對您的思念，在將來能成為有用的人。

目錄

圖目錄

表目錄

第一章 緒論

1.1 研究動機

在現今的網路通訊中，已經由有線網路連結擴展至無線網路的通訊，而無線網路主要由無線基地台和行動裝置組成，例如無線擷取點(Access Point)和 PDA。隨著 3G 以及 WiMax 時代的來臨，無線網路的發展成為將來的趨勢。

無線網路和有線網路最大的不同在於媒介存取與行動裝置的傳輸範圍限制，於基礎網路(Infrastructure Network)中，擷取點的無線媒介傳播的傳輸只能持續在一個範圍之內，若網路行動裝置移出擷取點所涵蓋的傳輸範圍時，便無法使用無線網路服務。此外擷取點的部署亦是一大問題，有些地區因為硬體或成本限制而無法架設擷取點，則會影響行動裝置的無線媒介存取範圍。

有鑑於基礎網路的限制，行動無基礎網路(Mobile Ad Hoc Network, MANET)便被提出以解決上述問題，此網路架構是由獨立的行動裝置所組成，具有自我組成的能力(Self-Organization)，可不須經由擷取點的支援運作，例如當傳送端節點想將資料傳輸到遠方接收端節點時，因為傳輸範圍的限制無法直接傳送至目的地，所以必須經由多點跳躍(Multi-hop)的方式由中繼節點續傳至接收端。

但是因為無線媒介的傳輸有一些安全機制的問題，所以本研究針對以下的問題發展出一套信任的機制。

(1) 無線網路易遭到有心人士的竊取，並將資料修改或藉由其他的方式對行動裝置做出攻擊。

(2) 在長期的通訊之下，不管是主動或是被動的攻擊，都會造成傷害。

(3) 行動無基礎網路是一種無中央管理的網路架構，故無集中管理的特性，有賴於發展分散式的安全管理架構才可確保資訊安全的運作。

(4) 行動無基礎網路是一個動態的拓樸架構，故節點的加入或離開都會動態的影響網路架構。

(5) 在現有的認證機制中，以 PKI 為基礎的認證機制因為是以中央控制憑證中心

(Certificate Authority)為主，故不適合行動無基礎網路。

(6) 受限於行動裝置的傳輸範圍，中繼節點可能因為省電而不將資料續傳，所以必須發展出一套機制以辨別節點的信賴程度。

本研究致力於提供行動無基礎網路在資料傳輸時的信任證據，藉由分散式的信任模式，讓每個節點都有各自的身分識別並將信任的情況表示，且不用線上的第三方做憑證的產生、發放與管理而可達成相互認證之目的，讓節點在進行資料傳輸時能夠判定中繼節點是否為信任的節點。

1.2 研究目標

以往在無線網路中的安全性研究中主要是以憑證中心(Certificate Authority)作為實體的憑證發給中心，網路節點藉由第三公正方的憑證來做基本的金鑰及資料交換基礎。但是在行動無基礎網路中，因為無線媒介範圍限制以及動態變動拓撲的關係，導致於實體憑證中心變的不可行。本研究之目標為在行動無基礎網路中建立分散式的信任機制，讓網路節點可以擁有屬於各自的信任證據(Trust Evidence)，並透過自我組成的方式管理。此外為了解決網路自私節點與惡意節點的問題，本研究期望除了建立個別節點互動後所評估之個別信任值之外，亦可整合各節點的信任值以求出此評估節點的總信任值，讓新進節點可以參考此節點之信任程度。節點在選擇中繼節點時除了可以參考個別信任值之外，也可藉由總信任值衡量來瞭解此節點和周圍節點互動的情況。

傳送資料需要耗費一定的資源，若沒有給予中繼節點一定的報酬，則中繼節點傾向不會轉送資料，故需要發展整體的信任值機制來對行動節點做評比，讓合作節點可以得到增加信任值的報酬，而自私節點和惡意節點則會因為和周圍節點的互動中被認定為不合作之節點，故會被減去一定的信任值。而在下一階段互動時，信任值高的節點的資料可以被優先傳遞並享有較好的服務品質，而信任值低的節點的轉送優先順序會較低，甚至轉送封包會被丟棄。本研究會用賽局來證明在行動無基礎網路中節點經由此信任機制會趨於合作的結果，並得到一定的報

酬。若節點選擇不合作則會漸漸被其他節點所忽略，故此節點雖然仍可在行動無基礎網路中存在，但是它的封包轉送要求會被其他節點拒絕，且無法和周圍節點互動。

本研究是以 Laurent Eschenauer, Virgil D,. Gligor, and John Baras 所提出的 On Trust Establishment in Mobile Ad Hoc Networks[6]為基礎，建構屬於行動無基礎網路節點的信任證據識別，並將信任機制包含至此識別，接著發展一套信任證據安全傳送及信任值衡量方式讓信任證據可以被網路節點存取。為了解決自私節點及惡意節點的問題，本研究可驗證經過信任證據的衡量後，可以基於 Vincent Buskens 的 Social Networks and Trust[3]證明不合作的節點會有一定的懲罰(Penalty)，且網路節點會朝向合作的結果。

1.3 研究方法

首先會就行動無基礎網路的架構與特性做討論，並根據所學之領域思考可研究之方向為何。在確定信任領域的研究方向後便針對研究之行動無基礎網路、信任證據、信任值、以及賽局做資料的蒐集和文獻探討，瞭解以往所著墨之部分和研究可改進的方向。根據文獻可確定研究之目的為發展一線上產生的信任證據識別機制，讓行動節點可以藉由自我組成管理周圍節點的識別，且針對互動之結果對節點產生評價，並經由可行性分析所有可能出現的問題及解決之方向。經由信任證據方法提出和不斷的修正後，將節點的識別號碼、公鑰、信任成員和信任節點之個別信任值、以及相關的雜湊函數包在整體的信任證據中，並在無行動基礎網路中產生、散佈、衡量及作區塊驗證。接著討論節點在網路中運作之情形，並利用賽局理論驗證節點必須藉由合作來得到最大之報酬，再加上以 NS2 模擬節點採用此信任機制和無採用時的比較，若驗證出現問題時亦可做修正，以得到結果分析並驗證。在整套研究方法完成後便可將結果文件化，且經由不斷驗證改進方法，讓本研究能帶出一定之貢獻。

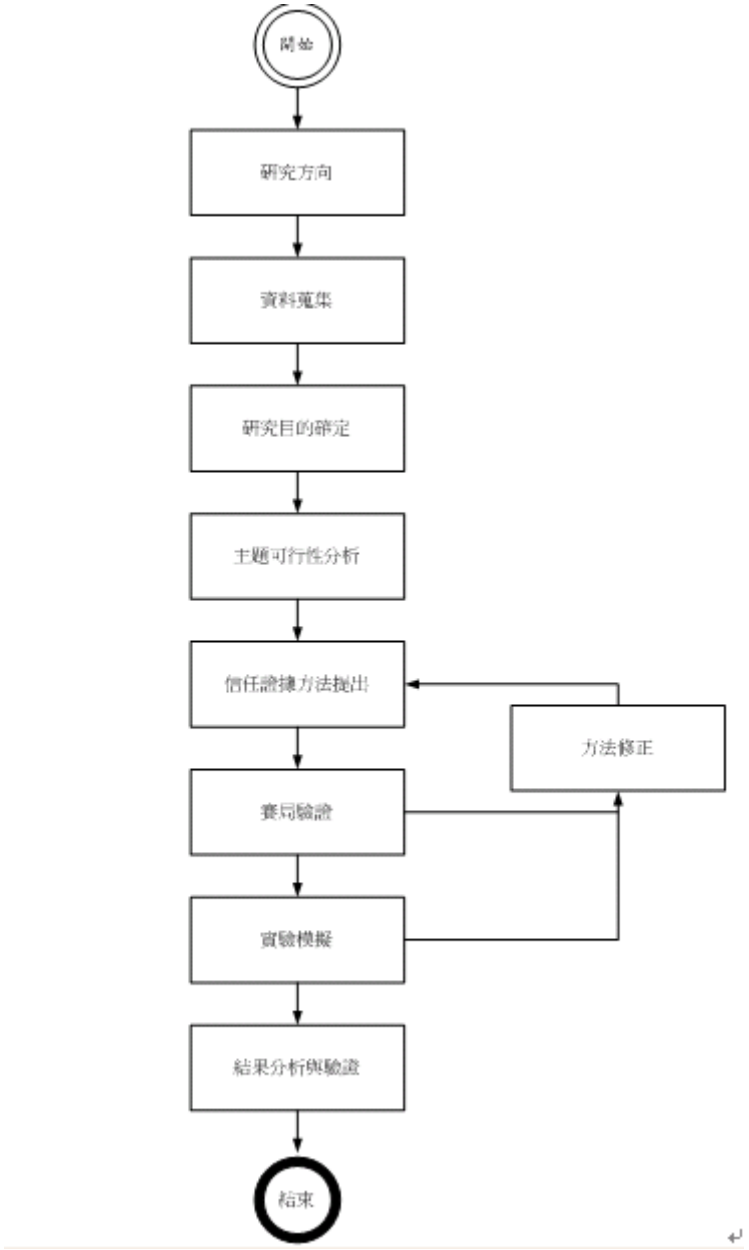


圖 1 論文研究步驟

1.4 研究架構

首先會就應用於軍事上的信任證據[6]衍生至行動無基礎網路中，並探討如何將身分識別、公鑰、信任成員、信任節點合併於信任證據中，最後研究相關的方法以抗衡自私節點和惡意節點的攻擊，亦即信任證據的衡量。節點在網路中的互動結果可以由各別信任值來反應出信任的情況，本研究會探討如何將各別信任值結合以及如何計算總信任值的方法。為了證明此信證據真正屬於該節點以及查證信任值的計算是否正確，可利用區塊驗證的方式來查證。根據信任值可利用賽

局理論分析節點的互動情況，並將連續封包傳送和相互封包傳送問題結合，若有節點採取背離策略時，也可探討尋找第三方節點的情況，和得到的報酬分析。

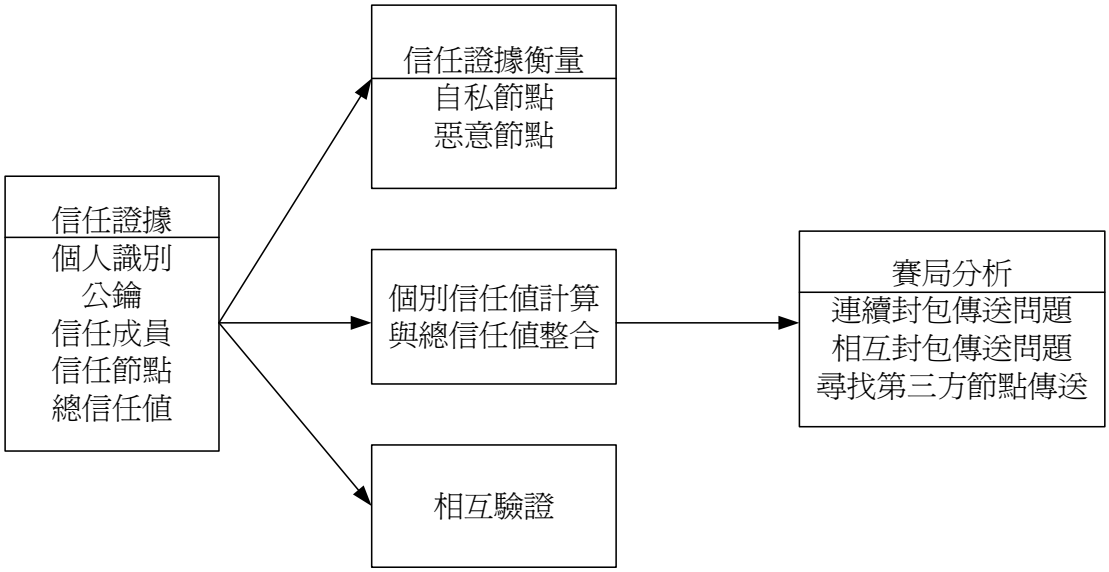


圖 2 研究架構

1.5 章節介紹

本研究分為六章節，第一章為本研究之簡介及研究方法之介紹，第二章會針對行動無基礎網路、公鑰管理、信任證據、信任值和賽局作文獻探討，第三章則會提出信任證據的方法和總信任值計算機制，第四會利用 NS2 對整體方法做分析及驗證。第五章利用賽局理論分析在信任證據的機制下，節點合作和不合作狀態對封包傳送之影響和報酬，並表達節點合作之最大利益結果。最後第六章總結本研究之結論及闡述未來可研究之方向。

第二章 文獻探討

2.1 行動無基礎網路

有線網路的發展已經趨於成熟的階段，雖然具有穩定及頻寬等一點存在，但是其連接工作站之不可移動性為其最大的缺點。隨著 IEEE 802.11 無線網路的發展，讓行動工作站可藉由自我組成來建構無線網路環境，並可透過多點跳躍的傳輸方式來達到通訊的目的。因為不需基礎設備的支援即可運作，故可用軍事或緊急救援行動，近年來已經運用於商業用途中，以達成區域服務導向的服務(Location Based Service)。

2.1.1 蜂巢式網路及行動無基礎網路

於行動通訊中最初的網路架構為蜂巢式網路(Cellular Networks)，其需要依靠基礎設備如基地台的支援才能運作，節點之間的必需經過單點跳躍(Single-hop)的方式接力完成。蜂巢式網路的優點在於基地台的存在可採集中的方式來做路由與資源的管理，以提供較安全與穩定的通訊服務，其缺點在於環境的建置需耗費成本且基地台若故障或節點移動到基地台通訊範圍以外則無法通訊。

因為 IEEE 802.11 的通訊協定制定，讓無基礎無線網路(Ad Hoc Wireless Network)的架構產生，其節點間透過多點跳躍(Multi-hop)的方式由多個節點的傳遞來完成資料傳輸，由於無基礎行動網路缺乏基地台的存在，使得路由與資源的管理必須採取分散的方式來處理。行動無基礎網路亦包含了無線網狀網路(Wireless Mesh Networks)以及無線感測網路(Wireless Sensor Networks)，無線網狀網路的節點之間都會有鏈路連結存在，而無線感測網路可以讓感測節點(Sensor)在特定的領域應用且在網路環境存在。

圖 3 的蜂巢和行動無基礎網路圖[13]可以闡述其中的關係，除了上述所提的網路之外，若網路架構包含兩者或網路架構可連接兩不同的網路，則稱為混合無線網路(Hybrid Wireless Networks)。

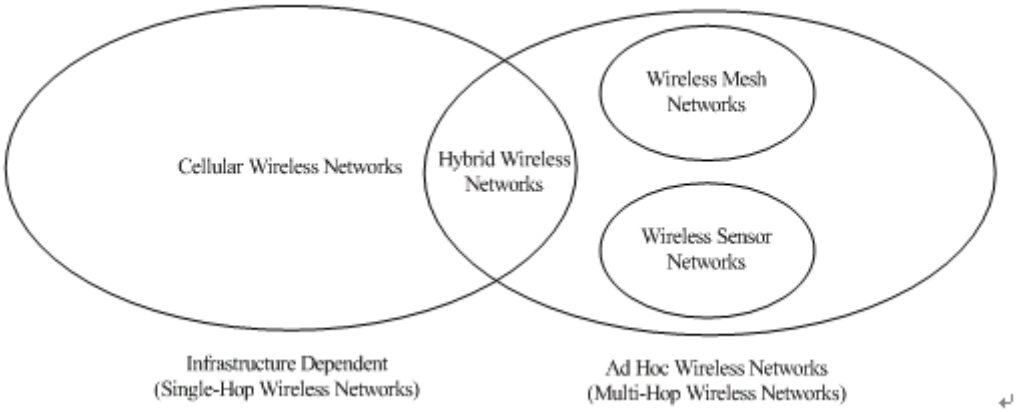


圖 3 蜂巢和行動無基礎網路

表 1 針對了蜂巢式網路以及行動無基礎網路做比較，由結果可知本研究適合動態架構且建立時間短的行動無基礎網路，所以在往後的研究都是基於行動無基礎網路之下發展不同的應用。

表 1 蜂巢式網路與行動無基礎網路比較

	蜂巢式網路	行動無基礎網路
架構	固定式架構	動態架構
主要目的	最大化通話接收率	最短路徑傳送
資源管理	集中式	分散式
頻寬管理	保證頻寬	共享無線電頻道
資料交換	線路交換	封包交換
無線鏈結	單點跳躍	多點跳躍
路由方式	簡單	複雜
環境建置成本	高	低
環境建置時間	長	短
應用領域	手機通訊及 3G	軍事及救援

2.1.2 行動無基礎網路的特性

根據上表所比較的特性可知，行動無基礎網路的兩大特性包含了動態拓璞

(Dynamic Topology)、多點跳躍(Multi-hop)、以及自我組成能力(Self-Organization)，以下針對此三大特性詳述。

動態拓樸起因於無基礎行動網路的通訊節點具有移動性，這些通訊節點可隨時進入或離開網路環境並在網路環境中任意的移動。為了滿足節點移動性的需求，這些節點往往具備有限的運算能力或電源供應，並且使用無線網路作為傳輸媒介。

多點跳躍可讓節點之間的通訊可藉由任何介於兩個節點之間的數個節點的協助來完成，因此封包傳遞路徑的選擇較為彈性但也因此較為複雜。由於行動無基礎網路缺乏基地台的存在，使得路由與資源的管理必須採取分散的方式來處理。

最後一個重要的特性為自我組成，在同一網路中節點可動態組織與維護網路，其中可透過鄰近節點發現(Neighbor Discovery)、拓樸組織(Topology Organization)、以及拓樸重新組織(Topology Reorganization)來達成。鄰近節點發現階段可讓節點藉由 Beacon 獲取周圍節點資訊並維護和紀錄環境資訊。至於在拓樸組織階段時，每個節點都會蒐集整個或部分網路的資訊以維護拓樸資訊。最後在拓樸重新組織階段時節點可依據節點移動情況、節點毀損、惡意行為和自私行為來更新拓樸資訊，其更新方式為定期更新或觸發更新。

2.1.3 行動無基礎網路的應用

由於行動無基礎網路不需任何基礎設備的支援，且具有網路環境建置需求成本低與速度快的特性，因此可用於軍事或緊急救援行動等，並應用商業用途中以提供便利的生活。

在軍事用途方面，無基礎行動網路特別適合用來作為軍隊作戰時通訊的媒介，由於在敵軍領土建立基礎設備來協助通訊幾乎無法立即辦到的，此時無基礎行動網路就可做為即時的通訊方式，此外對於大型的軍事單位，可藉由衛星所提供的全球定位系統(Global Positioning System, GPS)來使無基礎行動網路的路由

與資源的管理運作更有效率。

又因為 PDA 及筆記型電腦的普及使得無線網路和 GPS 的使用更趨頻繁，例如定位服務和以區域為基礎的服務產品銷售近年來都處於上升的狀態。但是無線網路的移動性以及訊號廣播的特性讓無線存取安全產生疑慮，故必須制定一套信任機制以維護無線網路的封包傳送安全。

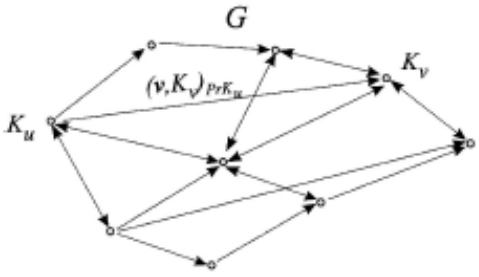
2.2 行動無基礎網路之公鑰管理

在有線網路中，公鑰及憑證的產生主要是由第三公正(Third Party)方的中央控制伺服器所發給，並可做資料驗證之工作。然而在行動無基礎網路中，網路節點是以分散式的分佈並具有動態的拓樸架構，使得線上的憑證中心(Certificate Authority)不可行，故需要建立以自我組成為基礎之公鑰管理機制，但是因為沒有公正方做安全性之驗證，讓公鑰的正確性產生質疑。Srdjan Capkun, Levente Buttyan, and Jean-Pierre Hubaux 建立了完全公鑰自我組成管理系統[4]，藉由使用者控制系統的安全設定以做憑證的驗證工作。

Step 0: 使用者初始化個別的公鑰/私鑰配對。

Step 1: 使用者發出公鑰憑證。

當使用者初始化公鑰憑證後，會附加有效時間(Valid Period, T_v)，憑證在有效時間內才有效，等過了有效時間後使用者必須重新初始化公鑰憑證。接著節點會建立更新(Updated)與非更新(Nonupdated)貯藏庫(Repository)，然後在行動無基礎網路中運作，所以會產生憑證圖(Certificate Graph G)，如圖 4 所示。



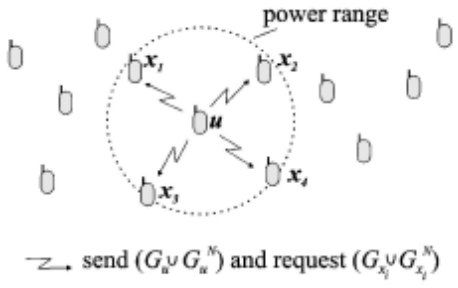
Step 1. Issuing of public-key certificates
(creation of the certificate graph *G*)

圖 4 公鑰憑證發佈圖

使用者 u 可以藉由間接通道的資料傳輸相信使用者 v 的公鑰 K_v 屬於使用者 v，使用者 v 可把他的憑證資訊和公鑰利用數位簽章的方式發給使用者 v。

Step 2: 節點進行憑證交換。

節點會發送一定傳輸範圍要求來搜集周圍節點憑證並創造非更新的憑證貯藏庫。

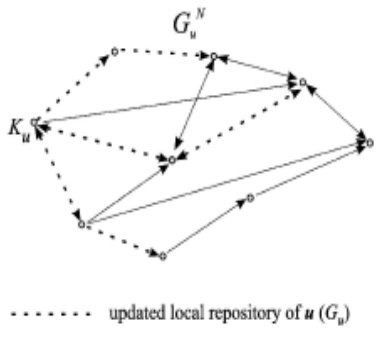


Step 2. Certificate exchange

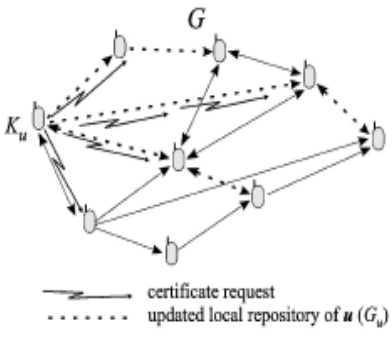
圖 5 憑證交換圖

Step 3: 節點建造更新憑證貯藏庫。

可利用兩種方式更新，第一種方式為和周圍鄰居驗證圖通訊以獲得新的憑證。第二種方式則是利用貯藏庫建構演算法利用接力的方式將憑證貯藏庫的憑證資料更新。所以在公鑰的傳遞當中亦包含了節點的憑證資訊，若有惡意節點假造公鑰並宣稱此公鑰為特定節點所發給時，周圍節點可利用本身儲存的貯藏庫憑證資訊或利用接力的方式向原節點求證，便可發現此公鑰非原節點所發出，故可確保公鑰的來源真實性。



Step 3a. Node u constructs its updated repository from G_u^N



Step 3b. Node u constructs its updated repository by communicating with other nodes

圖 6 憑證更新

經由完全自我組成的公鑰管理，每個使用者可以為他的公鑰憑證負責並傳遞屬於他本身的憑證給網路其他節點，並可藉由憑證圖的建構達成高效率的憑證傳遞，讓認證功能再行動環境下能快速進行且可偵測出不一致和錯誤的憑證。

2.3 信任證據與信任值

在社會化的互動中，因為每個人皆為獨立的個體，為了在團體環境中生存，人和人之間必須透過互動以得到利益，但是如何選擇較有信譽的人合作是個重要的課題，故信任在此社會便產生了，人們藉由信任的關係獲取雙贏的結果，並排除自私且具惡意的人。行動無基礎網路中節點也有其類似的信任關係，節點需要有信任的周圍節點以代傳封包，並需要幫助其他節點傳送封包以建立互信的關係。Vincent Buskens 定義了網路節點的信任特徵[3]。

(1) 信任是節點受其他節點信任的程度。

(2) 被信任的節點可以發揚信任(Honor Trust)或欺騙信任(Abuse Trust)。

(3) 當一節點信任另一節點，它可以請求被信任節點幫忙轉送封包，同時若此被信任的節點請求原先節點幫忙轉送封包時，此原先節點會幫忙轉送封包。

(4) 在信任關係建立後，會有一段時間讓節點做互動，當節點背離時原先節點可以不對此背離節點採取信任的態度;相反的若被信任節點合作時，原先節點會享受到發揚節點所得到的利益。

2.3.1 信任證據

身分認證在無行動基礎網路中是網路使用者表達自己識別的基礎方式，以讓周圍節點確認往後將要通訊的對象，又為了衡量通訊節點的信任程度，可以將節點識別和信任程度相互結合，以達到資料轉送的安全。此外亦可將認證的概念用於數位簽章，藉由簽章讓文件確認為該方所簽署，以達成不可否認性之要求。然而在行動無基礎網路中的節點為互相獨立且為完全自我組成的架構，所以必須擬定一套包含身分識別、憑證資訊、以及信任機制的整體信任證據方式，並在線上

(On-line)做個別節點信任證據產生、散佈、衡量、以及驗證。

信任證據最先用於軍事聯盟中[6]以表示友軍的識別標誌。在圖 7 的軍事應用實例中，假設英國(UK)和美國(US)互為友邦並擁有互相信任關係(Peer Trust Relation)。當英國步兵團(UK1)戰爭失敗退守至山洞以請求支援時，可利用信任證據識別(軍旗、軍服或其他識別証明)以證明 UK1 是友軍，並透過 GPS 告知其所在位置。這時英國指揮總部便可透過互相信任關係告知美國的指揮部以尋求支援，美國指揮部便可告知其步兵團(US1)前往指定地點救援。

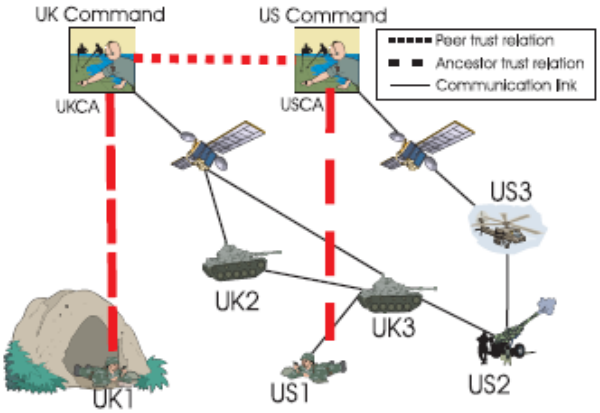


圖 7 信任證據軍事應用實例

基於以上的軍事運用，在行動無基礎網路中便更近一步的拓展信任證據，以重新定義網路節點中的信任證據。

(1) 信任證據是一個憑證，可表示節點的獨一性(Uniqueness)及特性(Characteristics)。

(2) 信任證據可以是一個識別、公鑰、所在位置和獨立的安全資產。

(3) 信任證據需要政策及衡量標準以建立其信任度。

(4) 信任證據在傳送時需要用節點的私鑰加密並有一段有效期限。

信任證據需被:

(1) 在網路節點中被產生、儲存、保護。

(2) 當需要時要動態路由至目的。

(3) 經由信任關係而線上(On The Fly)衡量動態證明。

(4) 在線上(On-line)衡量信任關係時，此信任關係是短期(Short-term)的並是以點

對點的方式衡量。

2.3.2 信任建立

倘若節點希望在行動無基礎網路中被其他節點所信任，且想要信任一中繼節點，則可以藉由信任建立(Trust Establishment)來達成。信任的建立可由系統蒐集客戶端(Client)的信任證據、定義信任政策，並基於以上兩者建立信任標準(Trust Level)。在信任建立時可針對信任政策(Trust Policy)、環境情況(Environment Context)、信任證據(Trust Evidence)、以及名譽(Reputation)來計算節點的信任值，以作為資料傳輸的節點選擇參考[20]。在信任政策中，是由管理者定義系統的安全判定方式以作為信任模式的衡量準則。而在環境情況中，包含了節點在環境的互動結果，例如頻寬、資料延遲、資料抖動等參數。信任證據則是節點的憑證和行為紀錄的真偽來改變信任值的大小。最後名譽是利用存取控制、加密、信任磋商、信任名譽衡量、信任授權及其他的衡量紀錄，最後將此四種衡量方式綜合評估已決定節點的信任程度。由下圖可知，當客戶端要求存取資源時，伺服器可由特定資源定義的信任政策和信任證據特性了解其需要驗證的信任模式為何。接下來便可利用信任特性取得相對的信任衡量資格、環境情況、行為、及名譽，來衡量是否信任此節點，若證據不足則可在蒐集其他的證據。

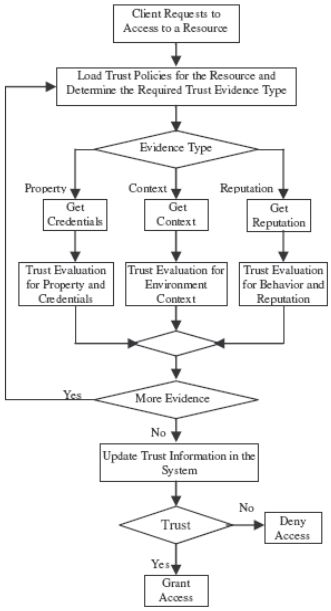


圖 8 於信任模式中信任建立之邏輯流程

於遍佈式計算環境中，因為行動化以及節點的動態性、不確定性、以及彈性讓信任建立的政策需要進行調整。當系統沒有客戶端資訊和第三方資訊時，需要進行信任溝通(Trust Negotiation)，使得客戶端和系統逐漸地揭露它們的證件以達成存取控制協定。而當系統信任客戶端時，它可以給予客戶特定的權利，這就是信任授權(Trust Delegation)的機制。

Kui Ren, Tieyan Li, Zhiguo Wan, Fen Bao, Robert H. Deng, and Kwangjo Kim 提出一套信任建立的機制[15]，基於每個節點都有各自的公鑰/私鑰以及節點註冊時其識別和公鑰都會由一私密的處理中心(Secret Dealer)儲存之假設，在信任建立後節點會由私密中心得到私密短列表(Secret Short List)，其中記載註冊節點的識別和公鑰集合(ID, P_k)。然而在行動無基礎網路中節點亦會散佈私密短列表以建立信任鏈結(Trust Chain)，由圖 9 可知在鏈結圖 G(V, E)於節點 i 包含了公鑰集合(ID, P_k)、認證期間以及以節點 i 之私密金鑰簽署的簽章。然而每個現存的成員節點皆可發起 k 個憑證。左圖為 k = 1 之情況，其組成的圖形為強健連結憑證圖，以傳遞的方式將憑證送出。而右圖則是 k = n - 1 的情況。這時組成的圖形為完全連接圖，每個節點都擁有週為節點的憑證資訊。

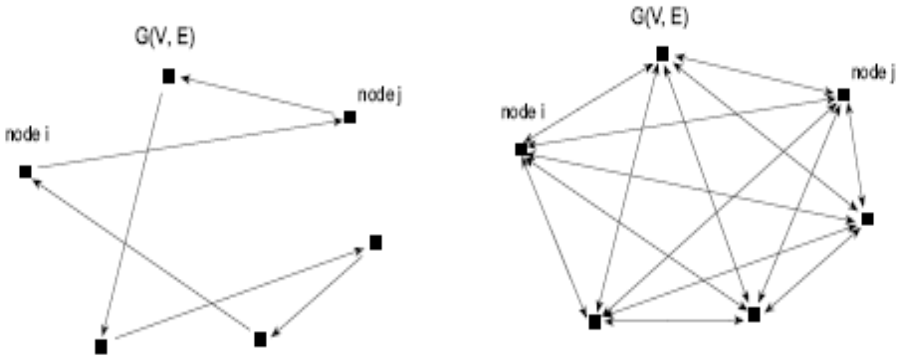


圖 9 於行動無基礎網路中不同 k 值之信任鏈

此方式雖然可以利用實體的私密中心做憑證的管理，但在行動無基礎網路中節點的產生、移動和離開的頻繁程度不適合此方式，故本研究所提出的方式必須

去除實體憑證中心而動態的建立信任關係。

2.3.3 信任關係

為了衡量特定對象節點之信任程度，可以利用信任值來衡量節點的信賴程度，並於固定時間更新，當信任證據被建立後，信任關係便產生於兩節點之間。信任關係包含了信任證據以及信任證據的衡量，圖 10 的信任關係運作中，當 B 決定是否信任 X 時，會要求 X 送出信任證據識別(X 的公鑰)並衡量 X 的信任程度，當 B 決定信任 X 後便會將 X 的信任證據儲存在資料庫中。而 A 也會經由相同的動作信任 B，如此一來整體的信任關係變產生了。

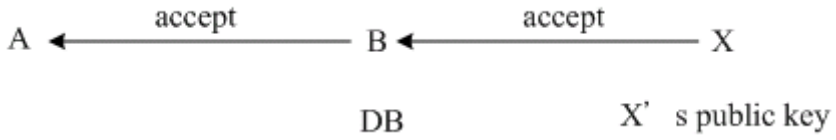


圖 10 信任關係運作

在信任關係中，越早建立的信任節點必須要有較強的信任值，並要有較持久(long-term)的信任程度。如圖 11 中 A 要使用他的衡量標準(Evaluation Metric)去決定 B 的信任程度時，必須確定 B 和 Y 的信任值以及持久性要強於 A 和 B 的信任關係，故才可進一步決定是否信任 B。

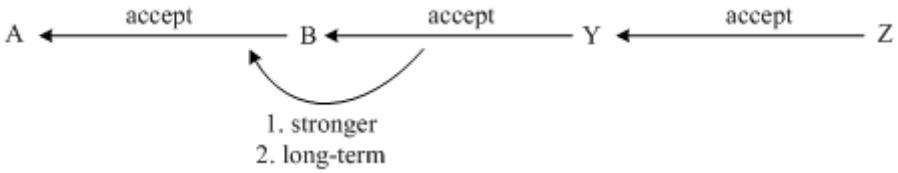


圖 11 信任關係特性

行動無基礎網路的信任關係建立時是以點對點的方式建立，並和信任架構獨立，並在線上建立，且具有快速建立及短期之特性。在信任關係信任中亦具有彈性並可支援不確定性及不完整的信任證據[6]。

2.3.4 信任散佈

惡意節點可能會產生或簽署錯誤的信任證據，故節點需透過信任關係去驗證信任證據的真偽，評價空間(Option Space)可以對節點產生評價[19]，每個評價空

間包含了信任值與可信度，其中前者為對目標節點的信任程度，後者為此信任程度的可信度，並使用 semiring 理論。

$$(t_{ik}, c_{ik}) \otimes (t_{kj}, c_{kj}) = (t_{ik} t_{kj}, c_{ik} c_{kj})$$

$$(t_{ij}^{p_1}, c_{ij}^{p_1}) \oplus (t_{ij}^{p_2}, c_{ij}^{p_2}) = \begin{cases} (t_{ij}^{p_1}, c_{ij}^{p_1}) & \text{if } c_{ij}^{p_1} > c_{ij}^{p_2} \\ (t_{ij}^{p_2}, c_{ij}^{p_2}) & \text{if } c_{ij}^{p_1} < c_{ij}^{p_2} \\ (\max(t_{ij}^{p_1}, t_{ij}^{p_2}), c_{ij}^{p_1}) & \text{if } c_{ij}^{p_1} = c_{ij}^{p_2} \end{cases}$$

圖 12 semiring 路徑評價

其中 $(t_{ij}^{p1}, c_{ij}^{p1})$ 代表節點 i 沿路徑 p1 對節點 j 的評價，可信度較高的信任值才會被採信，若可信度相同時則採取信任值較高的節點。

於 Peer-to-peer 網路的信任散佈可利用推薦機制加以整合[10]，定義衡量信任或不信任的標的物稱之為 Principals，並可被認證及以公鑰加以識別。信任(Trust)可視為預測 Principal 未來的行為標準，並可以建立在證據(Evidence)之上，然而衡量的方式要觀察先前的互動情況以及推薦情況來決定節點是否可以被信任。下圖的推薦架構資料流在剛開始可由節點蒐集推薦情況(Gather Recommendations)，並由基於證據(Evidence)將信任散佈給周圍節點，當資料傳送時會依據信任值來決定傳送至某節點的概率(Likelihood)，這時要考慮本益比(Costs / Benefits)及相關的風險(Risk)，接著便可作存取控制決定(Access Control Decision)，最後可將互動的結果及發現(Observation)以推薦的形式發出(Emit Recommendation)。

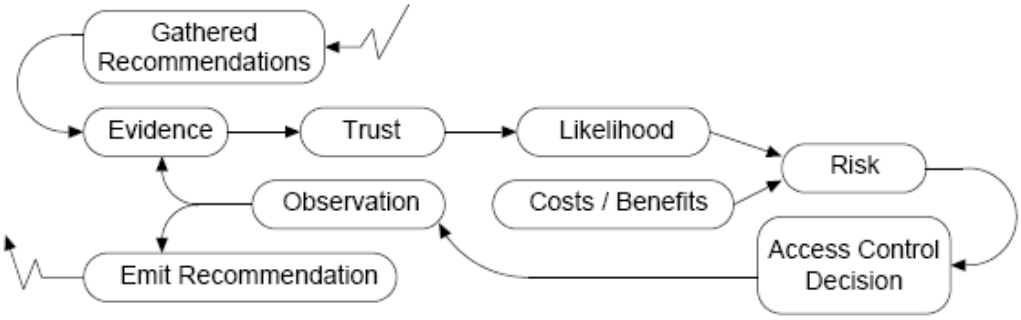


圖 13 推薦架構資料流

個人的行為可記錄於行為剖繪格式(Behavior Profile Format)中，表 2 的紀錄包含了觀察者(Witness)、被觀察者(Subject)、被觀察者所採取的行動(Action)、行動的成功率(Success Rate)。

表 2 行為剖繪格式

Subject	Witness	Action	Success rate	Local Outlier	Global Outlier
ALICE	EMILY	ECOM	50%	0	1
ALICE	CLAIRE	" "	10%	0	0
ALICE	DAVID	" "	95%	1	0
ALICE	BOB	" "	0%	0	0
ALICE	FRED	" "	10%	0	0
ALICE	***Overall***	ECOM	6.7%		

螞蟻演算法亦可作為行動無基礎網路中信任證據散佈的基礎。在以螞蟻為基礎隻信任散佈(Ant-based Evidence Distribution) [11]方法中，藉由放出代理者(Agnet)去找尋網路中的路徑並包含信任證據，故可由代理者代為攜帶傳出。表 3 的節點憑證表顯示了周圍節點的憑證資訊，每一行為一個憑證資訊，記錄著傳往周圍節點的機率，機率越大代表節點被信任的程度越高，其傳向它的可能性也越高。

表 3 節點憑證表

	Neighbors			
	N_1	N_2	.....	N_m
$Cert_1$	P_{11}	P_{12}	.....	P_{1m}
$Cert_2$	P_{21}	P_{22}	.....	P_{2m}
...	...	...	...	...
$Cert_n$	P_{n1}	P_{n2}	.....	P_{nm}

表 3 有 n 個憑證，以 $Cert_1$ 為例，P_{11} 代表了搜尋憑證 1 時傳往鄰近節點 N_1 的機率，P_{12} 則是搜尋憑證 1 時傳往 N_2 的機率，以此類推。其中 $\sum_{i \in N_k} P_{ni} = 1$，$N_k$ 為節點 k 的子集合。

倒退的螞蟻會搜集環境資訊以更新節點憑證表，根據[6]可得到以下的機率

更新。

$P_i(n) = \frac{P_i(n-1) + \Delta p}{1 + \Delta p}$ 。

$P_j(n) = \frac{P_j(n-1)}{1 + \Delta p}$ ，其中 $j \in N_K, j \neq i$ 。

i 是倒退螞蟻所傳回經過的鄰近節點，Δp = k / f(c)且 k 為大於 0 的常數值。成本 c 可以表示成節點傳送的任意代價，例如傳封包所經的節點數(Hop Count)、獲取憑證所需的延遲、節點頻寬消耗、以及電力。f(c)是以成本 c 的非遞減函數，以 $f(c) = \frac{a \times L}{\sum_{i=1}^{L} Q_i}$ 表示，其中 a 為常數，L 為總封包傳送所經節點數{$N_1, N_2, \ldots, N_L$}且 L 大於 0，並有相對的信任值{$Q_1, Q_2, \ldots, Q_L$}。故可知當 L 越大，f(c)越大，則往此節點傳的機率越低，故不傾向傳往此節點。然而當 Q 越大，f(c)越小，則往此節點傳的機率越高，故會傾向傳往此節點。

為了要確保信任證據以及包含的信任值不會被惡意節點所更改，本研究可用數位簽章的方式來保證信任證據的私密性、完整性及不可否認性。當節點要離開網路時，會產生並散佈撤銷證據(Revocation Evidence)以註銷產生的信任證據，此為撤銷憑證(Revocation Certificate)之方式。節點亦可產生對立證據(Contradictory Evidence)來對其他節點表達不同的意見，若對立證據存在其中，則此節點的信賴程度也就降低許多。

2.3.5 信任值計算與衡量

信任值的計算方式可利用權重方式，藉由定義信任值參數並基於參數在社會網路中的重要性給予不同的重要程度，最後經由加總計算出信任值的改變值[14]。

Trust Value: $TV = \sum_{i=1}^{n} [W_x(i) * T_x(i)]$

根據上述針對自私節點和惡意節點所衍生的信任值判定方式，可定義增減信任值之計算方式:

$TV = W_{FR} * T_{FR} + W_{BW} * T_{BW} + W_D * T_D + W_{Routing} * T_{Routing} - W_{Blacklist} * T_{Blacklist}$

其中的參數表示為:

- FR : Forward Rate
- BW : Bandwidth
- D : Delay Time
- Routing : 包含了 route request、route reply(ACK)、route error 所算出的 routing rate。

當信任建立後，節點可經由多點跳躍(Multi-hop)的方式將封包傳送至目的端，且可避免將封包轉送到惡意節點，

評價空間(Opinion Space)可作為信任值評估後的結果審核[19]，以回顧先前做的信任值評估是否正確且真實的反應節點的行為。信任值(Trust Value)是節點(Issuer)評估標的物(Target)的信任程度，當信任值越高代表標的物是合作節點且可以信任。而確信值(Confidence Value)則是評估信任值的正確性，當確信值越高代表節點和標的物互動的時間月久且和次數越多，最重要的是此信任值越能代表真實情況，圖 14 為信任值與確信值的組合表示，故可視為評價空間。

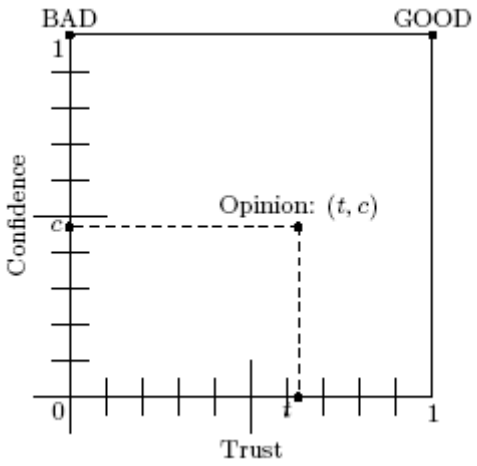


圖 14 評價空間

有了評價空間了以後，信任衡量系統便可運作，下圖的運作情形中首先會搜集地域性監視情況、互動情況、和公鑰交換情況，故可獲得實體鄰近節點的直接

信任證據。根據以上的評鑑，可做鄰近節點的信任衡量並得到信任值，再根據多重來源及目的端的路徑評估得到目的端的間接信任值。最後可由直接與間接信任值作信任決策以選擇節點傳送封包，並評價信任值的正確性以作為下次傳輸的參考。

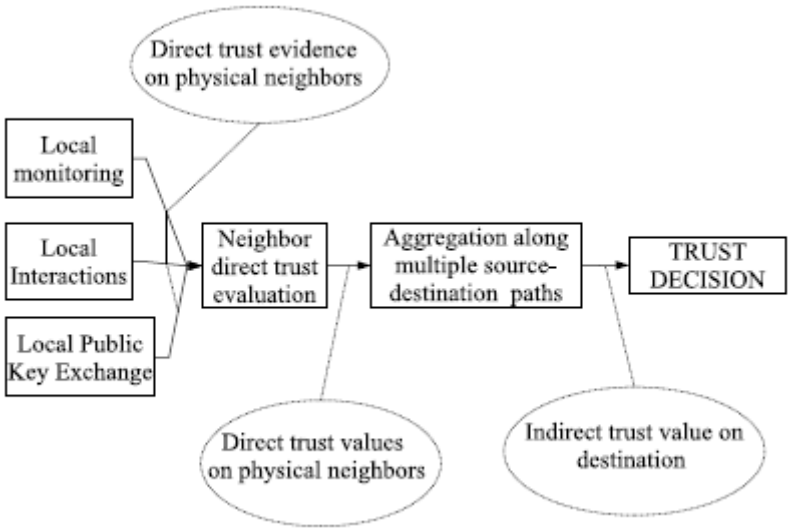


圖 15 信任衡量系統運作

2.4 賽局理論

2.4.1 賽局理論

賽局理論是一個交互作用的決策理論，可以用來預測一群參與者之行為互相影響之結果，即單一參與者之行為會影響其他參賽者最後報酬[17]。然而賽局包含了標準式賽局(Normal Form Game)與擴展形式賽局(Extensive Game)，標準式賽局中所有參與者都可以同時去選擇他們的行動，而擴展形式賽局可以讓參與者在不同的期間選擇行動。

定義 1 標準式賽局(Normal Form Game):

(1) 參與者集合(Set of Players):存在 N 個參與者，並被排列在一組合集中 I, $I \overset{def}{=} \{1, 2, \cdots, N\}$。在本研究中參與者包含了 $n_1, n_2, r_1, \ldots, r_n$ 等節點。

(2) 行動集合(Set of Actions):每一位參與者 i, $i \varepsilon I$，存在行動集合(Action Set) A^i，

表示參與者所有可能的行動集合。令 $a^i \varepsilon A^i$ 表示參與者 i 採取之特定行動。故可定義 $A^i \overset{def}{=} \{a_1^i, a_2^i, ..., a_{k_i}^i\}$，其中 k_i 為參與者 i 所能採取行動之數目，A^i 即為某特定參與者可以採取的行動集合和結果 a。而在本研究中包含了傳送封包(Forward)與丟棄封包(Drop)兩種行動。

(3) 結果(Outcome): 令 $a \overset{def}{=} (a^1, a^2, \ldots a^i, \ldots, a^N)$ 為每個參與者選擇行動之集合，故可將此行動集合定義為賽局的結果(Outcome)。本研究中的傳送封包與丟棄封包的組合即為賽局的結果。

(4) 報酬集合(Set of Payoffs): 因為參與者會選擇不同的行動組合以得到相對的獎賞(Reward)，並扣除相關的付出成本(Cost)，故定義報酬為獎賞和付出成本的差值(Payoff = Reward - Cost)。而每一參與者 i 都會有其報酬函數 π^i，並可將每一賽局所得到的結果對應至一個實際函數 $\pi^i(a)$。

賽局理論可以被分為兩大類，分別為非合作(Non-cooperate)及合作(Cooperative)[9]。

定義 2 非合作(Non-cooperate)賽局: 賽局會模擬每參與者所可能採取的行動對賽局的影響，且參與者不會去尋求互相合作的結果，故需要將每個參與者分離並探討可能的行動。

定義 3 合作(Cooperative)賽局: 探討不同參與者的組合對賽局的影響。

此外賽局亦分為完全資訊(Perfect Information)與非完全資訊(Not Perfect Information)兩類[9]。

定義 4 完全資訊(Perfect Information)賽局: 每個參與者能夠理解賽局的不同結果對他的影響。

(1) 參與者能夠獲取其他參與者之資訊。

(2) 參與者可能的行動。

(3) 在行動組合後所得的報酬。

在本研究中的賽局是完全資訊之非合作賽局，因為在無行動基礎網路信任機

制中，每個參與者的行動結果都已經被明確的定義，並有相對的報酬。又因為網路中存在自私節點以及惡意節點，故節點有可能背離(Deviate)合作關係，故本研究可針對可能背離的情況設計出相對的懲罰，讓節點趨向於合作的狀態。

2.4.2 納許均衡

賽局的形成可以擁有各種不同的結果，而藉由探討所有各種不同的結果是不切實際且無法做任何的預測，故可發展分析方法並將結果所小至一範圍內，使得均衡結果(Equilibrium Outcome)能夠被決策者所用。理想狀態中參與者做一個行動只會得到一個結果，故此均衡狀況為唯一(Unique)。但是在均衡狀況中行動組合常常不是唯一，且有可能發生均衡不存在之情況。

先前已經定義了賽局的結果集合為 $a \overset{def}{=} (a^1,\ldots a^i,\ldots, a^N)$，若除了參與者 i 之外，其他參與者的行動集合為 $a^{-i} \overset{def}{=} (a^1, \ldots, a^{i-1}, a^{i+1}, \ldots, a^N)$。綜合以上的定義可知結果 a 可被表達成 $a= (a^i, a^{-1})$。

首先定義優勢行動的均衡[17]，假設參與者在實際的情況下所會採取的行動便稱為優勢行動。

定義 5 優勢行動(Dominant Action)：假設對於參與者 i 之特別行動 $\tilde{a}^i \in A^i$ 為優勢行動。故實行 $\tilde{a}^i$ 可使參與者 i 獲取最大的報酬，而其他所有參與者所能採取的行動為 a^{-i} 。

$\pi^i(\tilde{a}^i, a^{-i}) \geq \pi^i(a^i, a^{-i})$ ，對於每一 $a^i \in A^i$ 。

$\pi^i(\tilde{a}^i, a^{-i}) > \pi^i(a^i, a^{-i})$ ，至少一個行動 $a^i \in A^i$ 。

賽局理論中可以發展出一均衡概念，此均衡可以選擇一個合理的結果，假設無參與者發現他背離此均衡是有利的，而此均衡為所有其他參與者在納許結果下不背離採取之策略。

定義 6 納許均衡(Nash Equilibrium)[16]：在賽局之結果組合中，定義結果

$\hat{a} = (\hat{a}^1、\hat{a}^2、...、\hat{a}^N)$，對於每個$\hat{a}^i \in A^i$且 i =1, 2, …, N，稱此結果為納許均衡。

為了要找尋納許均衡，可從檢查參與者是否單方面背離而獲利，故要認定行動結果不為納許均衡的條件為證明有其中一位參與者可藉由背離到不同的行動獲得更大的報酬。總之在檢查賽局時無發現沒有任何參與者可藉由背離獲得更大報酬時，就可以斷言發現了納許均衡解。然而納許均衡不一定是唯一，賽局中也有可能出現多數的納許均衡。此外賽局中也有納許均衡不存在之情形發生，即在結果中至少有一個參與者發現背離均衡是有益的。

定義 7 柏拉圖最佳化(Pareto-Optimal)[16]: 對於參與者 i 之特別行動$\tilde{a}^i \in A^i$為柏拉圖最佳化。故實行$\tilde{a}^i$可使參與者 i 獲取最大的報酬，而其他所有參與者所能採取的行動為a^{-i}。

$\pi^i(\tilde{a}^i, a^{-i}) \geq \pi^i(a^i, a^{-i})$，至少一個行動$a^i \in A^i$。

2.4.3 標準型式賽局

在非合作賽局中，依照資訊完整的程度和參與者是否參考他人的選擇情況調整可分為四種賽局形式，分別為完全資訊下之靜態賽局(Static Games of Complete Information)、完全資訊下之動態賽局(Dynamic Games of Complete Information)、不完全資訊下之靜態賽局(Static Games of Incomplete Information)、以及不完全資訊下之動態賽局(Dynamic Games of Incomplete Information)[9]。

定義 8 標準型式賽局(Normal Form of Representation): 參與者在賽局中同時選擇行動組合的結果可以用表格的方式呈現，並把組合行動所會得到的報酬顯示在相對應的欄位，讓參與者參考不同的決策所得到的結果。

定義 9 完全資訊下之靜態賽局(Static Games of Complete Information): 在靜態賽局(Static Game)中，所有參與者可以同時決定策略的情況，而完全資訊(Complete Information)則代表參與者的效用函數對於所有的參與者而言皆是公眾的知識(Common Knowledge)。故參與者可以利用效用函數來分析其他參與者的

回應以決定依行動組合，而此行動組合可以最大化本身的報酬。

囚犯兩難(The Prisons' Dilemma)是完全資訊下之靜態賽局中最具代表性之賽局實例，表 4 的標準形式賽局將囚犯兩難的組合呈現。

表 4 囚犯兩難標準形式賽局

嫌犯二 / 嫌犯一	坦白	不坦白
坦白	-6, -6	0, -9
不坦白	-9, 0	-1, -1

此例子敘述有兩名嫌疑犯被警察逮捕，由於沒有足夠的證據證明他們有罪，故兩名嫌疑犯被分開至不同偵訊室偵訊，在偵訊時告知各嫌疑犯其偵訊結果會影響最終的判刑。在表格中，若兩名嫌犯均坦白罪行則會被各判 6 年的徒刑，如果有一方先坦承罪行而另一方卻否認涉案，則坦白的一方會被判 0 年徒刑，而不坦白的一方會被判九年徒刑。最後若雙方皆不坦承犯行，則兩人各被判一年徒刑。

藉由納許均衡可以預測參與者選擇行動之可能的結果，故只要有一參與者有偏離之誘因則此策略組合就不是納許均衡，若嫌疑犯認為選擇坦白會得到較多的效益，則可預測嫌犯會做出坦白的決策。以下便針對四種不同的情況討論行動組合是否為納許均衡。

情況一:兩嫌犯均坦白。

在嫌犯二坦白的情況下，可知嫌犯一可選擇兩種策略，若坦白其報酬為-6，而不坦白則為-9，所以嫌犯一的最佳反應為坦白，故無偏離之誘因。同理嫌犯二亦會選擇坦白，所以雙方皆坦白為一納許均衡解。

情況二:嫌犯一坦白但嫌犯二不坦白。

在嫌犯一坦白的情況下，可知嫌犯二可選擇兩種策略，若不坦白則為-9，而坦白其報酬為-6。又$-9 < -6$，故嫌犯二有偏離之誘因，所以此情況不為一納許均衡解。

情況三:嫌犯一不坦白但嫌犯二坦白。

在嫌犯二坦白的情況下，可知嫌犯一可選擇兩種策略，若不坦白則為-9，而坦白其報酬為-6。又-9＜-6，故嫌犯二有偏離之誘因，所以此情況不為一納許均衡解。

情況四:兩嫌犯均不坦白。

在嫌犯二不坦白的情況下，可知嫌犯一可選擇兩種策略，若不坦白其報酬為-1，而坦白則為 0。又-1＜0，所以嫌犯一的最佳反應為坦白，故有偏離之誘因，所以雙方皆不坦白不為一納許均衡解。

定義 10 完全資訊下之動態賽局(Dynamic Games of Complete Information):動態賽局代表了參與者可以觀察其他參與者決定的行動後才做出決策，故完全資訊下之動態賽局可讓參與者觀察上一階段的結果做下一階段的參考。

以投資者問題為例，有兩名投資者各投資 D 並存入銀行中，銀行會將前納入長期投資中，若有在投資進入成熟期之前有投資者將錢領出時，只有 2r 的錢可被領出，其中 D＞r＞D/2。然而如果投資進入成熟期後，投資者可領回較多的錢，即有 2R 的錢可被領出，其中 R＞D。假設第一階段投資是處於不成熟的情況，而第二天為成熟之情況。

在第一天的投資情況中，若兩方投資者皆提款則兩者各分 r 元。若有一方提款而另外一方不提款，則提款的一方可以得到 D 元，不提款的一方可得到 2r - D 元。最後若雙方都不提款，則代表投資者希望能夠進行長期投資，故會進入下一階段的投資中，其標準式賽局如表 5 所示。

表 5 第一天投資情況標準形式賽局

投資者二 / 投資者一	提款	不提款
提款	r, r	D, 2r-D
不提款	2r-D, D	下一階段

由於在第二天的投資進入了成熟階段，所以兩位投資者總共可拿到 2R 的金

錢。若兩方投資者皆提款則兩者各分 R 元。若有一方提款而另外一方不提款，則提款的一方可以得到 2R-D 元，不提款的一方可得到 D 元。最後若雙方都不提款，則最終的投資終止後雙方各會拿到 R 元，其標準式賽局如表 6 所示。

表 6 第二天投資情況標準形式賽局

投資者二 / 投資者一	提款	不提款
提款	R, R	2R-D, D
不提款	D, 2R-D	R, R

定義 11 不完全資訊下之靜態賽局(Static Games of Incomplete Information)：參與者可以同時選擇不同的策略但至少有一個參與者不知道他人的效用函數。例如在密封式競價中，每個競標者雖然都知道自己的效用函數，但是卻無法知道他人的效用函數，故可視為同時決定價格策略，而此行動不一定是對參與者最有利的，有可能會導致高估的情況發生。

定義 12 不完全資訊下之動態賽局(Dynamic Games of Incomplete Information)：參與者可以觀察其他人的策略後才做決策，但是參與者不一定會全盤了解其他人的效用函數。最常見的例子為求職市場訊號(Job-Market Signaling)，公司起初在招募新人時會針對求職者的學歷來決定是否錄用此求職者。

本研究會針對完全資訊下之靜態賽局做節點合作及違背做討論，並在任一節點違背合作策略後，進入完全資訊下之動態賽局以找到第三方節點代傳資料。

2.4.4 擴展形式賽局

先前已對標準形式賽局做明確的定義並敘述其種類，其中的特性為參與者被限制於相同時間內選擇行動，然而在某些情況中參與者可再不同期間行動且可超過一次以上，這時賽局便將此互動稱為擴展形式賽局[17]。

定義 13 擴展形式賽局(Extensive Form Game)：

(1) 有一組 N ≥ 1 的參與者，以 i 表示，其中 i = 1, 2, …, N。

(2) 擴展形式賽局包含了參與者、策略、報酬、以及移動的順序。

(3) 擴展式賽局為一樹狀圖，包含起始節點、其他決策節點、終止節點、和連接每一決策節點到後繼節點的分支。其中起始節點(Root Node)是參與者最初做決策的節點，其他決策節點則可讓參與者在特別的時間點以參與者為名選擇不同的行動。當參與者採取了一系列的決策後，賽局就會終止，並以終止節點(Terminal Node)表示最終行動組合的結果，且對於每一參與者都會有一報酬。以上節點都會被分支(Branches)所連接，並將行動組合聯繫至終止節點。

(4) 擴展式賽局包含了階段(Stage)的概念，其定義為參與者在一時間點所做的互動(Interaction)組合，在每個階段中每一個參與者都會選擇各自的行動。故參與者在 t 階段的欲選擇的行動會參考至 t - 1 階段的賽局，所以先前做決策所得到的結果及報酬皆會反應至參與者且被參與者作為下一次選擇行動的參考指標。

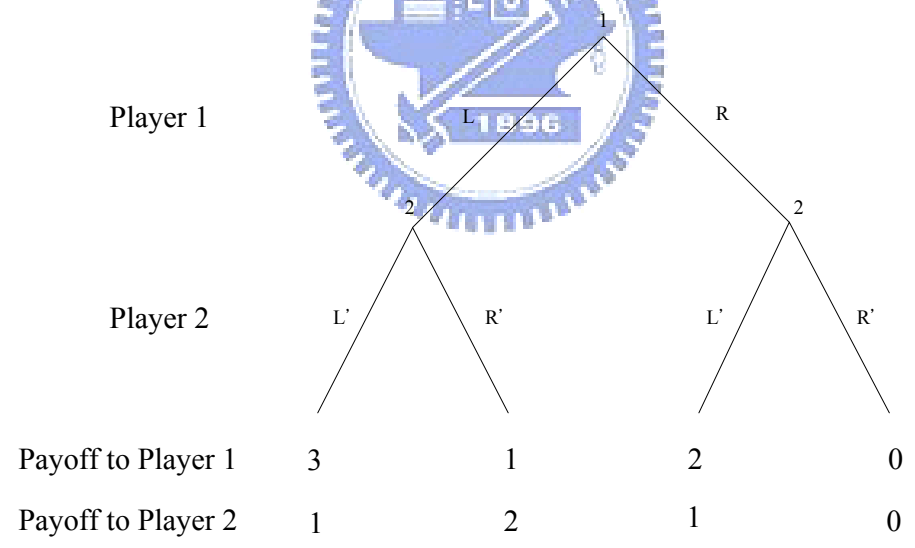


圖 16 一階段擴展式賽局實例

圖 16 為一階段擴展式賽局的實例，由上圖可知參與者一(Player 1)可以在集合 $A^1 = \{L, R\}$選擇一個左或右的行動(a_1)，參與者二(Player 2)可以先行觀察參與者一所採取的行動後從集合 $A^2 = \{L', R'\}$，賽局結束後參與者一會得到報酬 $\pi^1(a^1, a^2)$，參與者二也會得到一報酬 $\pi^2(a^1, a^2)$。例如若參與者一和二都選擇左的行動，則參與者一會得到 3，參與二會得到 1; 若有一參與者選擇左而另一參與者選擇

右，則選擇左的參與者會得到 1，右的會得到 2; 最後若雙方皆選擇右，則會各得到 0 的報酬。

2.4.5 賽局於無線網路中之應用

在無線區域網路中，因為節點傳送的電力及範圍有限，故無法保證來源節點可直接將封包傳送至終端節點，所以必須請求周圍節點以接力的方式將封包傳至終端節點，傳送封包需要消耗節點一定的電力及資源，所以節點會傾向不幫忙轉傳封包。為了要在行動無基礎網路中讓轉送封包的機制能夠持續運作，所以需要發展獎勵制度讓節點認為幫助轉送封包可以獲得一定的報酬，當此節點認同獎勵制度後便合作，故在下一階段時若此節點需要請他人轉送封包時周為節點也會優先幫忙轉送封包。在探討此信任機制之前先討論在行動無基礎網路可能遇到的封包傳送問題[8]，分別為連續封包傳送問題(Sequential Packet Forward Problem)和相互封包傳送問題(Mutual Packet Forward Problem)。

首先在最單純的情況中，封包會由依序的方式由傳送端(se)經由中繼節點(n_1和 n_2)將封包接力傳送至接收端(r)，而 n_1 和 n_2 有可能因為各種因素將封包丟棄，故以賽局理論探討此可能發生合作或背離的情況稱為連續封包傳送問題(Sequential Packet Forward Problem)，如圖 17 所示。

圖 17 連續封包傳送問題

假設封包傳遞成功後節點會得到值為 1 的報酬，而傳送封包需要耗費 C 的成本，其中 $0 < C << 1$。由圖 18 整理出的連續封包傳送問題標準式賽局可知又四種情況發生，當 n_1 及 n_2 都採取幫忙轉送封包的策略時，兩個節點都會各得到 1-C 的報酬; 又 n_1 決定轉送封包，而 n_2 卻採取不合作的態度，故封包無法傳送至接收端，則 n_1 會因為沒達成任務而得不到報酬，且損失了傳送封包所需的成本

C，n_2 因為將封包丟棄所以得不到任何報酬；若 n_1 採取不合作的態度即將封包丟棄，則 n_2 無法做是否轉送封包的決定，故 n_1 會得到 0，而因為 n_2 無法做決策所以沒有參與到賽局中，n_2 也會得到 0。

表 7 連續封包傳送問題標準形式賽局

n_1 \ n_2	Forward	Drop
Forward	1-C, 1-C	-C, 0
Drop	0, 0	0, 0

以下利用納許均衡判斷方法來分析不同情況分析節點的策略，並檢視周圍節點是否有偏離的誘因，若沒有此情況發生則會得到納許均衡解且再實際網路運作中節點也會朝向此一策略做轉送封包與否的決定。

情況一: n_1 及 n_2 兩節點均轉送封包。

在 n_2 節點答應轉送封包的情況下，n_1 可以選擇兩種策略，若轉送封包則可得到 1-C，不轉送則為 0，所以可知 n_1 最佳反應為轉送封包，且無偏離之誘因。同理 n_2 及也會轉送封包，由此可知雙方皆轉送封包為一納許均衡解。

情況二: n_1 轉送封包但是 n_2 丟棄封包。

在 n_1 轉送封包的情況下，可知 n_2 可選擇兩種策略，轉送封包則可得到 1-C，不轉送則為 0。又 0 < 1-C，故 n_2 有偏離之誘因，所以此情況不為一納許均衡解。

情況三: n_1 丟棄封包但是 n_2 轉送封包。

在 n_1 丟棄封包的情況下，n_2 無法選擇兩種策略，亦即 n_2 無法參與至賽局中，所以此情況不為一納許均衡解。

情況四:兩節點皆丟棄封包。

在 n_2 節點採行封包的策略下，n_1 可以選擇兩種策略，若轉送封包則可得到 -C，不轉送則為 0，所以可知 n_1 最佳反應為丟棄封包，且無偏離之誘因。而在 n_1 決定丟棄封包時，n_2 不會有任何的決策產生，所以 n_2 無偏離之誘因，經推論可知雙方皆丟棄封包也是納許均衡解。

然而連續封包傳送標準式賽局中，n_1 及 n_2 節點皆傳送封包為柏拉圖最佳化，因為在行動組合中，沒有別的行動組合優於 n_1 及 n_2 節點皆傳送封包。

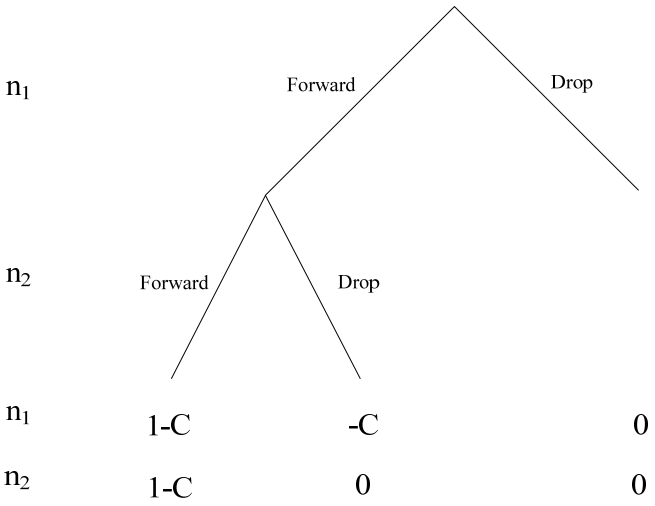


圖 18 連續封包傳送擴展式賽局

根據標準式賽局分析，可將結果轉換成一階段的擴展式賽局，除了可把兩節點的策略顯示出來之外，相關的報酬也可在終端節點表示，如圖 18 所示。

上述例子為連續傳送封包問題，封包的傳送為單一方向轉送，所以 n_2 會有丟棄封包的傾向。然而在行動無基礎網路中封包的傳送有可能是雙向傳輸，在某一時間點時節點可能會要求周圍節點轉送封包，也有可能會收到周圍節點要求己方轉送封包的訊息，所以要考慮相互封包傳送的情況，故稱此狀況稱為相互封包傳送問題(Mutual Packet Forward Problem)。由圖 19 可以了解到 n_1 可能會要求 n_2 把封包轉送到 r_1，故此時 n_2 就扮演著中繼節點的角色。同理可知 n_2 亦可能會要求 n_1 把封包轉送到 r_2，故此時 n_1 就扮演著中繼節點的角色。

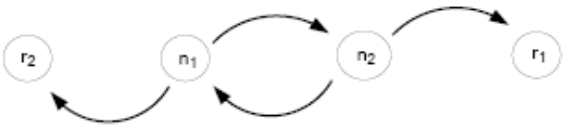


圖 19 相互封包傳送問題

同上述的方法，可以得知相互封包傳送問題的標準式賽局，在圖 19 中當 n_1 及 n_2 都採取幫忙轉送封包的策略時，兩個節點都會各得到 1-C 的報酬；又 n_1 決

定轉送封包，而 n_2 卻採取不合作的態度，故封包無法傳送至接收端，則 n_1 會因為沒達成任務而得不到報酬，且損失了傳送封包所需的成本 C，n_2 因為將封包丟棄所以可以將資源節省起來做別的事，所以 n_2 可以得到 1 的報酬；若 n_1 採取不合作的態度即將封包丟棄，則 n_2 也是會耗費成本 C，故 n_1 會得到 1-C，而 n_2 會得到 1；最後若雙方皆決定丟棄封包，則雙方既沒有傳送封包也沒有得到好處，所以雙方節點都沒得到任何報酬。

表 8 相互封包傳送問題標準形式賽局

n1 \ n2	Forward	Drop
Forward	1-C, 1-C	-C, 1
Drop	1, -C	0, 0

以下也利用納許均衡判斷方法來分析不同情況分析節點的策略，以找出最可能的行動組合。

情況一: n_1 及 n_2 兩節點均轉送封包。

在 n_2 節點答應轉送封包的情況下，n_1 可以選擇兩種策略，若轉送封包則可得到 1-C，不轉送則為 1，所以可知 n_1 最佳反應為丟棄封包，且具備了偏離之誘因。同理 n_2 及也會丟棄封包，由此可知雙方皆轉送封包不為一納許均衡解。

情況二: n_1 轉送封包但是 n_2 丟棄封包。

在 n_2 丟棄封包封包的情況下，可知 n_1 可選擇兩種策略，n_1 丟棄封包可以得到-C 的報酬，轉送封包則可得到 1-C，。又-C < 1-C，故 n_1 有偏離之誘因，所以此情況不為一納許均衡解。

情況三: n_1 丟棄封包但是 n_2 轉送封包。

在 n_1 丟棄封包封包的情況下，可知 n_2 可選擇兩種策略，n_2 丟棄封包可以得到-C 的報酬，轉送封包則可得到 1-C，。又-C < 1-C，故 n_2 有偏離之誘因，所以此情況不為一納許均衡解。

情況四:兩節點皆丟棄封包。

在 n_2 節點採行丟棄封包的策略下，n_1 可以選擇兩種策略，若轉送封包則可得到-C，不轉送則為 0，所以可知 n_1 最佳反應為丟棄封包，且無偏離之誘因。而在 n_1 決定丟棄封包時，n_2 也可以選擇兩種策略，所若轉送封包則可得到-C，不轉送則為 0，所以可知 n_2 最佳反應為丟棄封包，且無偏離之誘因，經推論可知雙方皆丟棄封包是納許均衡解。

然而在此相互封包傳送標準式賽局中，n_1 及 n_2 節點皆傳送封包為柏拉圖最佳化，但是雙方皆傳送封包不為納許均衡解。

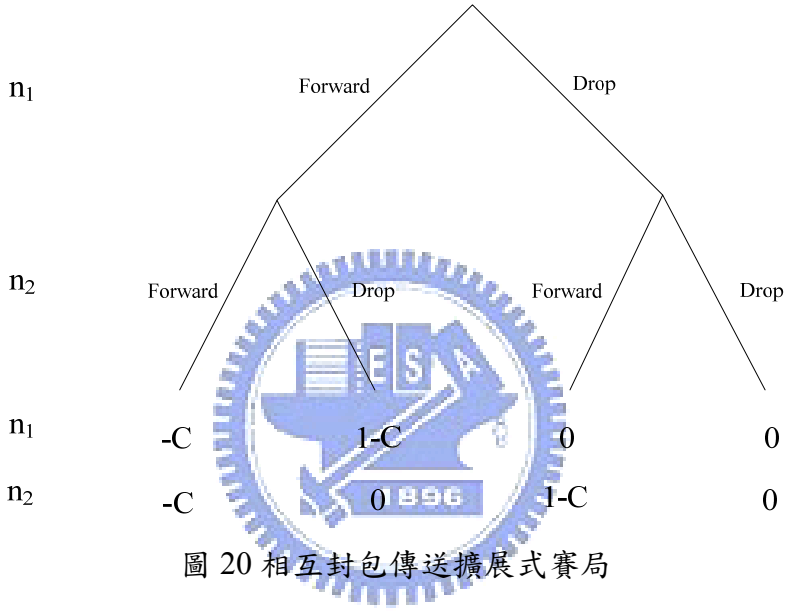


圖 20 相互封包傳送擴展式賽局

根據標準式賽局分析，可將結果轉換成一階段的擴展式賽局，除了可把兩節點的策略顯示出來之外，相關的報酬也可在終端節點表示，如圖 20 所示。

社會網路讓節點選擇是否採取信任周圍節點的策略，使得賽局理論可以用在行動無基礎網路中並分析網路節點的行為，Vincent Buskens 定義了 Trustor 與 Trustee 兩者的關係[3]，圖 21 的一階段擴展式賽局詳述了節點間的信任關係。由起始節點觀之，Trustor 可以選擇採取信任或不信任的方式，此種選擇類似於 Trustor 節點在選擇周圍節點 Trustee 時，是否信任此節點而要求它轉送封包。若 Trustor 採取信任(Play Trust)Trustee 的策略時，Trustee 有兩種策略可供選擇，第一種為發揚信任(Honor Trust)關係，亦即幫助 Trustor 節點轉送封包，所以 Trustor 可以得到 R_1 的報酬，Trustee 則得到 R_2 報酬。反之如果 Trustee 採取欺騙信任(Abuse

Trust)的決策時，則 Trustor 可以得到 S_1 的報酬，Trustee 則得到 T_2 報酬。第三種狀況為 Trustor 不採取信任(No Trust)的措施，則雙方只會得到 P_1 及 P_2 的報酬，其中 $R_1 > P_1$，$R_2 > P_2$。

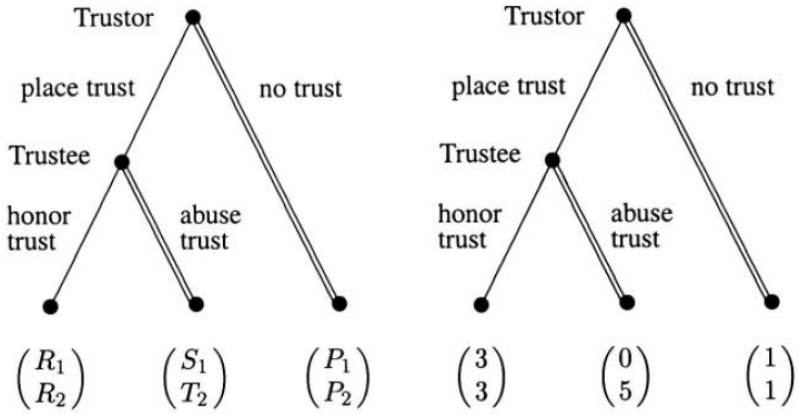


圖 21 信任擴展形式賽局

以上是針對資訊完整性的社會網路做信任賽局分析，但是在某些情況下資訊是呈現不完整的狀態中，所以必須仰賴本身經驗或藉由先前的互動關係選擇是否信任節點。在下圖的不完全資訊之信任擴展式賽局中，有 0.6 的機會走向壞的方向，所以在 Trustee 背離的情況下，Trustor 得到的報酬 S_1 會比較少。反之有 0.4 的機率賽局會走向較為信任的模式，這時若 Trustee 採取背離的策略，則 Trustor 得到的報酬 S_2 會略大於壞方向的報酬 S_1。經過整理後可得到此一階段的信任擴展形式賽局數狀圖，其中 $R_i > P_i$，$T_{2,1} > R_2$，$T_{2,1} > R_2$。

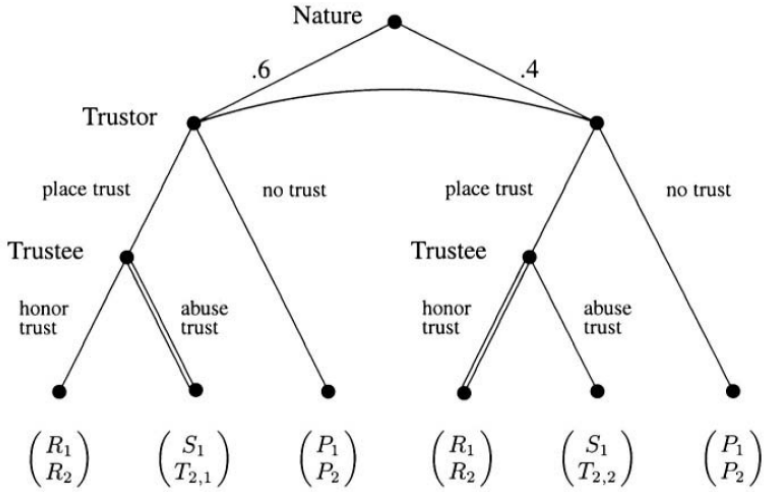


圖 22 不完全資訊之信任擴展式賽局

第三章 信任證據產生、散佈與信任值計算機制

先前對於信任證據的研究中，是以個別信任值評比方式來判別目的方的屬性，並有中央控制機制做資料的管理及傳送。而在行動無基礎網路(Mobile Ad Hoc Network, MANET)中，因為每個節點的電力傳輸範圍有限，無法藉由直接的資料傳送獲得遠方節點的資訊，故需要利用接力傳送來傳送資料。為了確保中繼節點是善意的節點且要避免自私節點和惡意節點作資料的轉送，故可以透過先前資料傳送時所得到的環境資訊了解節點互動的情況並給予信任值，在下一次傳送時便可利用信任值挑選最受信任的節點作資料的轉送。

此研究中針對行動無基礎網路提出一個分散式的信任證據機制，讓網路節點可以各自產生代表己方的憑證並擁有相關的信任識別，而不用中央管理端(如Certificate Authority)來控管，以在行動無基礎網路中作為節點的識別、傳送、衡量，故可在平行的網路架構中動態的運作且在封包傳送時可參考各別及總信任值以選擇合適的節點要求轉送。

3.1 問題定義

3.1.1 信任散佈問題

於信任的散佈中，雖然藉由資訊的傳送可以讓對方了解到傳播方的資訊，但是卻沒有建立一套身分認證的方式，所以接收方無法得知對方的身分，故無法相信對方的意圖及提供的資訊是否正確。本研究可針對信任證據的產生與散佈建立線上的身分憑證，讓信任值高的網路節點共同管理，當節點傳送己方的憑證時接收方可以透過區塊驗證已查證此節點的身份是否正確。

在以往的推荐機制中[10]，提及了如何將評鑑的信任值散佈，但是節點無法確定周圍節點所評鑑的信任值真正是由它們所評價的，且在信任值的傳送中也可能被攻擊者擷取並竄改相關的資訊。為了解決以上的缺點，本研究將身分憑證和

信任值包裝成信任證據，傳送前會將資訊透過雜湊函數(Hash Function)算出雜湊值(Hash Value)，在傳送階段會利用數位簽章的方式確保私密性、完整性、以及不可否認性，所以在信任證據的散佈可以確保傳送資訊的安全。

3.1.2 自私節點問題

因為在行動無基礎網路中，傳送封包資料會耗費節點一定的資源，例如電力、運算力等，所以有些節點會為了達到自身利益最大化的情形，選擇性的將其他節點要求轉送的封包丟棄，故此節點就成為了自私節點(Selfish Node)。自私節點的存在會讓傳送端無法將封包傳送至目的地，進而在接收不到 ACK 的情況下選擇別的路徑傳送封包。又當節點移動的情況下，因為先前沒有和一些周圍節點互動過，所以在選擇中繼節點傳送時會有一定的機率選擇到自私節點而耗費傳送資源。本研究藉由總信任值的參考讓傳送節點可以參考周圍節點和中繼節點互動的情況，以了解此節點先前是否採取合作的狀態，再選擇是否和此節點合作並要求轉送封包。

3.1.3 惡意節點問題

行動無基礎網路具有無線網路傳輸、節點移動、分散式資源管理以及電源管理的特性，所以會造成惡意節點(Malicious Node)假造路由資訊或使用大量請求路由封包以癱瘓節點和其傳輸效能。惡意節點會使用不同的攻擊方式讓行動裝置的傳輸效能降低，故可使用修改資訊、假造以及偽裝的方式做出攻擊，本研究可針對此攻擊因應出相對應的方式，並用信任值來表示攻擊所帶來的影響。

修改(Modification)是攻擊最常使用的方式，最簡單的方式為更改資料的內容，以讓接收端取得錯誤的資料且破壞完整性，在本研究中可利用數位簽章的方式達到資料的完整性。在 Black Hole 的攻擊模式[5]中，惡意節點會更改最佳路由路徑，並透過更改位址(Redirect)方式將封包導引至此惡意節點，故可搜集封包的資訊來達成攻擊的目的。其中最常見的是 Denial of Service(DoS)攻擊，在 DoS 攻擊中，攻擊者可利用跳板或發送路由請求以攻擊特定之節點，使得被攻擊方無

法處理其他合法的服務請求，並耗損其網路頻寬及電力。在 Grey Hole 的攻擊模式[5]中，是以丟棄封包的方式，把要求轉送的封包過濾不傳以避免花費電力傳送，本研究可以藉由計算封包傳送率針對 Grey Hole 攻擊做出有效因應，並調整信任值。最後則是關於繞徑之攻擊，惡意節點會傳送錯誤的繞徑訊息以混淆封包的傳送或造成長距離繞徑(Longer Route)，可利用延遲時間(Delay Time)計算封包從傳送端送至目的端的時間，以解決上述問題。

惡意節點亦會假造不屬於原先傳送節點的資訊以欺騙接收方，這時可利用數位簽章來確認此資訊是否為傳送端所傳送之正確資料，若經由查證發現中繼惡意節點偽造資訊時，可使用黑名單(Blacklist)記錄此情況並廣播至附近節點，以將惡意節點忽略。

3.1.4 個別信任值問題

以往的研究著重於個別節點對中繼節點的信任值衡量，此舉往往侷限於己方節點的衡量。但是當節點移動至新的區域且要和先前從未衡量過的節點互動時，無法使用個別衡量值做節點的參考，則和沒有採用個別信任值的環境無異。再者傳送節點雖然和中繼節點互動過並得到信任值衡量，可是如果此傳送端因為特定原因而有一段時間沒有和此中繼節點互動，當傳送節點經過長時間後希望重新和中繼節點互動，而此時中繼節點的行為及採行的策略可能會有所不同，故先前傳送端針對中繼節點的個別信任值衡量的參考價值便降低許多。

本研究建構於個別信任值的衡量，再經由信任證據的傳送得到周圍節點對此節點的個別信任值，然後計算出總信任值。如此一來不僅可參考各別的信任值，亦可得到周圍節點和中繼節點互動的情況，以選擇最適節點幫忙轉送。上述所提之問題亦可解決，原因在於傳送節點的個別信任值的參考價值雖然降低，但是可藉由周圍節點持續的對此中繼節點評估其信任值，故可以得到行動無基礎網路中節點最真實的互動狀況。

3.2 研究假設

在提出信任證據的管理之前，必須針對行動無基礎網路的特性並基於先前的研究提出一套假設，讓本研究可以在可靠的理論之下發展出具可信度的方針。假設包含了各自節點的資訊、信任證據、公鑰交換方式(Public Key Exchange Mechanism)、環境資訊等事先定義之基礎。

3.2.1 節點資訊

首先每一個網路節點都會有各自且唯一的識別號碼(ID_i)，此 ID 不會因為節點的增加或離開而有所重複，此外每個節點也會有各自的公鑰(Public Key, PK_i)及私鑰(Private Key, pk_i)，且有公開的雜湊函數(Hash Function, h())，如此一來節點可以擁有基本的識別資訊，並可做資料的加解密和數位簽章的功能，以達成資料私密性、完整性、不可否認性等安全要求。

3.2.2 信任證據

每個網路節點會擁有屬於各自識別的信任證據，信任證據中包含了節點的 ID、公鑰、信任成員(Trust Member, TM)、信任節點(Trust Node, TN)、總信任值(Total Trust Value, TTV)、以及其他節點的公鑰。其中信任成員為在行動無基礎網路中被其他成員所信任的節點資訊，故為他人的訊息。而信任節點則為己方信任或衡量過的節點訊息，故含有自己對周圍節點的衡量資訊。總信任值則是代表此節點經由周圍的節點信賴衡量後所算出的最終信賴值，故此總信賴值包含了不同節點對此節點的信賴描述，更能貼近此節點的互動情況及信賴程度。

3.2.3 環境資訊

節點在網路環境中交換資訊時會得到一些環境資訊，在衡量互動的信賴程度時，就可利用這些資訊做信任值的計算。環境資訊包含了傳送機率(收到 ACK 與未收到 ACK 的差異值與傳送封包的比值)、頻寬(Bandwidth)、延遲時間(Delay Time)、黑名單等資訊。其中黑名單資訊為當周圍的某一節點作出欺騙行為或重大危害傳送利益行為時，會由發現者公告此節點的行為，讓其他未和此惡意節點互動的裝置記錄此節點而大幅降低此節點的信任值，以忽略此惡意節點的存在。

在做信任值的瞬間計算時，信任證據及總信任值不會改變，此舉是會了確保在以上兩者的查詢值不會改變，而在計算完畢後才可填入新的信任證據及各別信任值。最後以上的資料交換中，節點都會採用數位簽章來傳遞資料，故可確保資料的私密性、完整性、以及不可否認性。

3.3 信任證據資料表示

每個行動無基礎網路節點都會擁有屬於各自的信任證據，以作為此節點的識別及特性描述，而在信任證據中含有此節點的 ID、公鑰之外，還包含了信任成員(Trust Member, TM)及信任節點(Trust Node, TN)。其中信任成員為此節點被其他節點信任的紀錄，其表示如圖 23 所示。

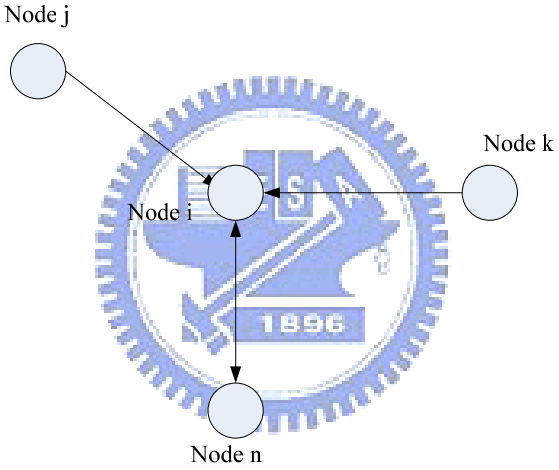


圖 23 信任成員表示關係

信任成員包含了信任此節點的識別號碼(ID)、公鑰(PK)、對節點的個別信任衡量值(TV_{ji})、信任時間(Timestamp)、到期時間(Expire Time)、節點所屬區塊(Block)、認可印章(Valid)。其資料表示和實例如整理成表 9。

表 9 信任成員資料表示

ID_j	PK_j	TV_{ji}	$Timestamp_j$	Expire Time	Block	$Valid_j$	Hash
002	PK_j	6	2007/1/24/19:00	2007/1/24/19:05	20	$Valid_j$	H()
003	PK_k	3	2007/1/24/19:00	2007/1/24/19:05	26	$Valid_k$	H()
008	PK_n	4	2007/1/24/19:00	2007/1/24/19:05	27	$Valid_n$	H()

於表格的屬性中，TV_{ji} 是周圍節點對中央節點的個別衡量，所以在 TM 中會有不同的 TV_{ji} 衡量信任值，讓 Node i 做整合計算的動作。Timestamp 則是周圍節

點做出信任值衡量的時間，並藉由 Expire Time 來決定此衡量值的有效期限，當過了此有效期限時，Node i 會要求重新衡量信任值。認可印章(Valid)則是用在驗證的部份，節點會做區塊求證的動作，當確認總信任值(Total Trust Value)運算正確時就會給予認可印章，代表個別節點認可此信任值，故在節點傳資料時就可依據認可印章確保總信任值是真正來自於個別節點且經過正確的運算。最後雜湊函數(Hash Function, h())會將先前的值計算出雜湊值，以確定值沒有被他人修改。

信任節點(Trust Node, TN)則是紀錄中央節點(Node i)對周圍節點的信任值，其目的有二。第一個目的是要在下一次選擇節點傳輸時參考信任值。第二則是用來做個別節點的信任值評估，以交付給被評估之節點做總信任值的計算。信任節點的衡量關係如圖 24。

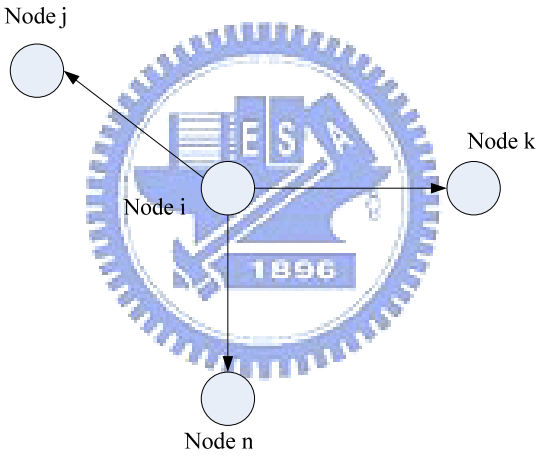


圖 24 信任節點表示關係

在本研究中不只針對個別節點的信任值衡量，也將整體的信賴值作計算，藉由受信賴的節點做信賴值的整合，不只可以讓新進的節點可參考中繼節點的信賴程度，也可以讓互動過的節點參考其他節點互動的結果，讓整體的網路繞徑的安全度更能提升。

信任節點的資料表示和信任成員之資料表示互相類似，都包含了信任節點的識別號碼(ID)、公鑰(PK)、對節點的個別信任衡量值(TV_{ij})、信任時間(Timestamp)、到期時間(Expire Time)、信任節點所屬區塊(Block)、認可印章(Valid)。其資料表示和實例如表 10。

表 10 信任節點資料表示

ID_j	PK_j	TV_{ij}	$Timestamp_i$	Expire Time	Block	$Valid_j$	Hash
002	PK_j	6	2007/1/24/17:00	2007/1/24/17:05	20	$Valid_i$	H()
003	PK_k	3	2007/1/24/18:00	2007/1/24/18:05	26	$Valid_i$	H()
008	PK_n	4	2007/1/24/19:00	2007/1/24/19:05	27	$Valid_i$	H()

和信任成員不同的是信任節點的信任值(TV_{ij})為中央節點(Node i)對周圍節點的評估信任值，此信任值可作為傳送考量和周圍節點的總信任值計算的基礎，而認可印章則為 Node i 的証明。

當節點接收到周圍節點全部的認可證明後，代表節點的總信任值的衡量和計算是正確的，故節點可利用雜湊函數(Hash Function, H())來將個人識別和總信任值(TTV_i)算出雜湊值，即定義 $H_i = h(ID_i, PK_i, TTV_i, \text{Expire Time})$。故當周圍節點要選擇中繼節點時，可以要求節點傳回它的信任證據，包含了總信任值和雜湊值，除了可以得到衡量此節點的認可印章以證明總信任值為正確之外，也可得到雜湊值以確保總信任值在互動過程中沒有被更改。

3.4 信任證據產生與散佈

本研究發展了一套信任證據的管理方法，讓信任證據可以在網路中經由傳送來得到節點的資訊，且不會被假造或修改。節點在經過社會化信任行為互動後，信任值高的節點可以透過信任值重新衡量的方式適時反應先前階段的互動結果。若中繼節點採取不傳送或做出對傳送節點不利的動作時，則此中繼節點會因為信任值的降低而成為不受信任的節點，故下一階段中若此節點要傳送資料時也會遭受其他節點的拒絕，直到此節點合作為止。

信任證據的管理方式可讓節點從進入行動無基礎網路時做一個初始化的動作，產生信任證據並散播至周圍節點。接著會做節點互動以及信任值評估及驗證，若節點為合作節點則會一直於網路中存在，最後節點可以藉由登出的方式離開網路，其流程圖可由圖 25 表示。

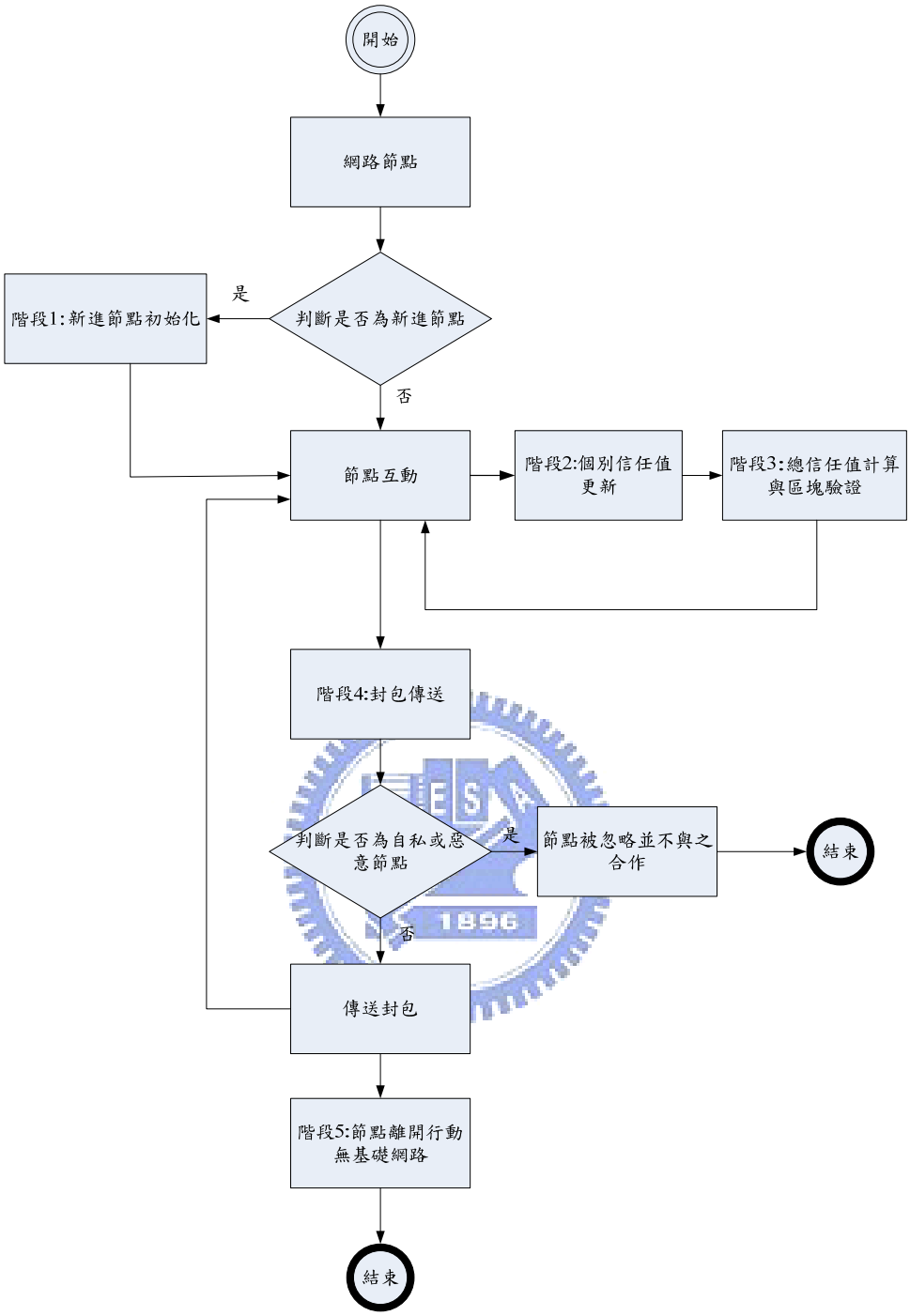


圖 25 節點信任證據產生與信任值衡量流程圖

在第 1 階段時節點會進入行動無基礎網路中，若節點為新進入節點，則會向周圍節點做信任證據初始化以成為行動無基礎網路中的節點，反之為舊有節點則直接進入第 2 階段。本研究會針對新進節點做信任值的初始化給予，並對行動無基礎網路中的節點做定期衡量的機制，讓節點可以信賴總信任值，以選擇高度信任的節點轉送資料，最後達到雙贏的結果。

在行動無基礎網路中，節點可經由社會化的網路互動得知周圍節點的信賴程度，故可以利用量化方式將信賴狀況轉換成信任值。在第 2 階段時節點會和周圍的節點作資料的轉送服務及互動，並由周圍節點做個別的信任值(Trust Value, TV)計算及更新。故在下一時間點要轉送資料時可依照信賴情況選擇信任的節點傳遞資料，且當周圍節點需要己方節點轉送資料時，可以藉由衡量傳送端的信任值決定是否幫它傳送資料，若傳送端的信任值過低，則可拒絕轉送封包。經由此機制可將不受信任的節點忽略，讓它處於孤立的狀態，並促使節點轉送資料，以讓整體網路能達到合作的狀況。

第 3 階段則是做信任證據散佈和主要被衡量的節點做總信任值(Total Trust Value, TTV)的衡量，並藉由區塊驗證以證明個別信任值是真正由周圍節點計算且總信任值的計算是正確的。

在第 4 個階段則是資料的實際傳送，節點會要求周圍中繼節點給予其信任證據，若傳送端節點先前沒有和中繼節點互動過，則會以周圍節點計算的總信任值作為比較值，即 $com_{ij} = TTV_j$。若傳送節點有和中繼節點互動過，節點則利用自己衡量的各別信任值和信任證據內的總信任值權重總和挑選權重信任值最大的節點代為轉送資料，即 $com_{ij} = \alpha * TV_{ij} + \beta * TTV_j$，並會增加它的個別衡量值以做為獎勵，故在下次此中繼節點要求轉送資料時，會優先替他轉送資料以做為獎勵。同樣的當傳送節點要將封包傳送給己方節點時，可以根據傳送端的總信任值決定是否代為轉送，若其總信任值小於最小可信任值時則不代為傳送。而如果同時有多方傳送端節點想要請己方節點轉送封包時，己方節點會根據總信任值以及個別信任值的權重總合取最大值優先傳送。

第 5 階段則為節點離開網路時的登出，以避免信任合作的誤判發生。當下次節點要進入行動無基礎網路時，可以重新的使用以往的設定值，故可確保先前合作所得到的信任值增加報酬可以延續。

以下便經由上述的階段中，根據節點進入行動無基礎網路後，其互動方式直到節點登出網路的協定以細部步驟詳述其運作方式，其各階段詳述如下。

階段 1:新進節點的初始化。

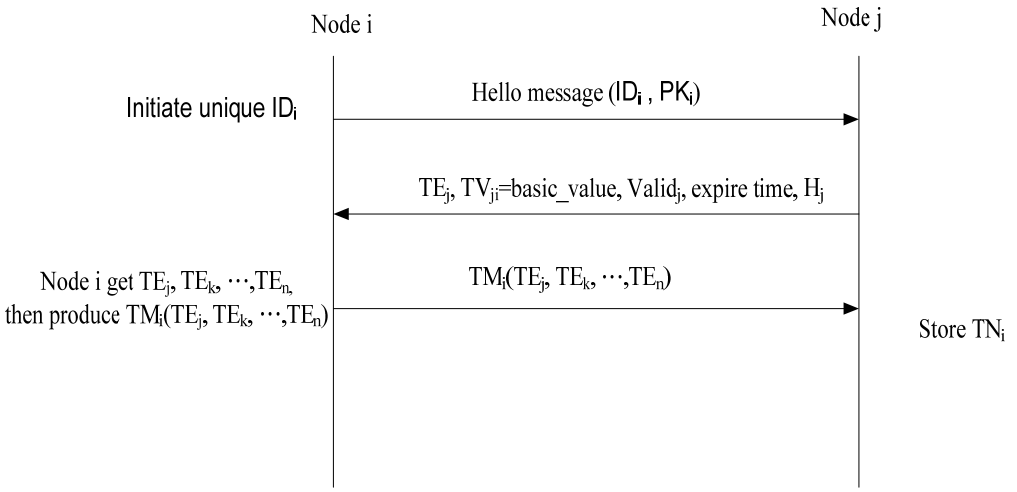


圖 26 新進節點初始化流程圖

(1-1):新進節點(Node i)送出 Hello Message，夾帶其 ID 及公鑰。

(1-2):周圍節點傳送信任證據，並給予基本信任初始值(basic_value)、認可印章、到期時間。

(1-3):Node i 將周圍節點之信任證據及初始化信任值儲存至信任成員(TM)。

(1-4):Node i 將信任成員傳送至鄰近區塊。

(1-5):鄰近節點將初始節點資訊儲存至信任節點(TN)中。

階段 2:個別信任值計算。

在此階段會由節點做個別信任值的衡量，其結果除了可以作為封包傳送節點的參考之外，也可作為總信任值計算的依據。本研究可利用封包傳輸率(Forward Rate)來評量節點轉送封包的程度，即採用收到 ACK 封包和未收到 ACK 封包的差除以傳送包的數量，並給予增減信任值。

$$forwardrate = \frac{SuccessACK - FailureACK}{SuccessACK + FailureACK}$$

在 Forward Rate 值為以下狀態時，給予不同的信任增減值。

- 0.3 以下:-1。
- 0.3-0.6:0。

- 0.6-0.9:1。
- 0.9-1:2。

因為考量到丟棄封包對節點重新找尋路由路徑的影響，故加重了遺失封包所造成的懲罰，讓節點更趨向於傳送封包。

除了衡量封包傳輸率之外，也可將路徑頻寬(Bandwidth, B)和傳送延遲(Delay Time, D)加以考慮，並透過權重分配計算出整體信任值的升降。

階段 3: 節點信任證據的散佈、衡量、總信任值計算、以及互相驗證。

在個別節點計算完各自的信任值後，本研究之第 3 階段是有關於信任證據的管理及衡量的部份。因為節點的互動影響了整體行動無基礎網路的狀態，故每隔一段時間後節點會搜集一定範圍內周圍節點對它重新的衡量值，故為(1)階段之舊節點信任證據衡量及總信任值計算，使得周圍節點要選擇節點傳送時不只會參照己方的信任值，也會參考不同節點的互動情況，以達到客觀的結果。為了要驗證個別信任值的擷取和總信任值的計算是正確的，於(2)階段會藉由區塊驗證以尋求周圍節點的証明，並由己方節點的計算以驗證總信任值的計算是正確的。

(1) 舊節點信任證據衡量及總信任值計算

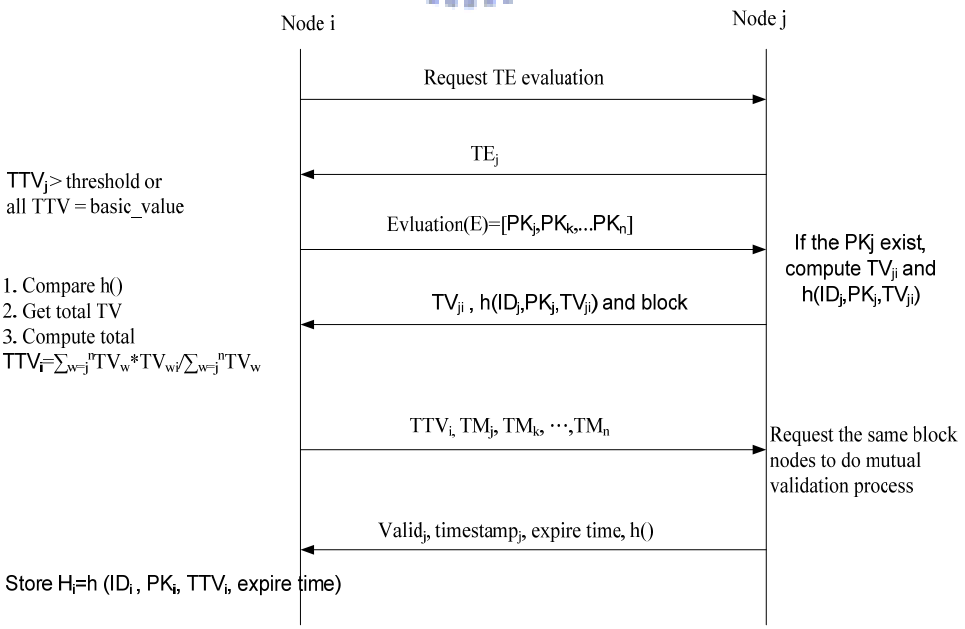


圖 27 舊節點信任證據衡量及總信任值計算流程圖

(3.1-1): Node i 要求信任證據衡量。

(3.1-2): 在鄰近區塊內的節點將它的信任證據傳回，其中包含了節點的總信任值。

(3.1-3): Node i 檢查節點之總信任值

(a) 若周圍節點皆為新進節點亦即總信任值皆為初始值，則讓全部的新進節點衡量它的信任程度。

(b) 若存在舊有節點，則在此節點中選取高信賴程度之節點作為衡量節點。然而周圍節點的總信任值必須高於一特定門檻值(Threshold)才可將衡量結果送回。此設計的用意在於避免惡意節點或自私節點故意將節點的信任值調整至不符合實際的互動表現，所以要讓具有一定可信度的節點衡量才具公信力。

(3.1-4): 將符合(2.2-3)條件節點之公鑰存入 Evaluation(E)，並向四周區域傳送。

(3.1-5): 周圍節點收到 Evaluation 後，檢查是否含有己方之公鑰，若有則將對中央節點的衡量信任值(TV_{ji})及它所屬的區塊位址(Block)傳回。

(3.1-6): Node i 接受後檢視以下條件

(a) 傳送的資料是否遭受更改，若有則要求重傳並查出其原因，若無則進行下一步驟。

(b) 將周圍節點對 node i 個別衡量的信任值取出。

(c) 計算總信任值，其公式為: $TTV = \frac{\sum_{w=j}^{n} TV_w \times TV_{wi}}{\sum_{w=j}^{n} TV_w}$，以信任值比例計算，信任值越高的節點擁有較高的權重。

(3.1-7): 將總信任值向周圍區塊廣播並註明信任成員，即信任值大於門檻值而可以衡量的成員。

(3.1-8): 當周圍節點接收到(3.1-7)的資料時，會依據相同的區塊作互相驗證。

(3.1-9): 若互相驗證通過，則將認可印章($Valid_j$)、衡量時間($Timestamp_j$)、到期時間傳回中央節點 Node i。

(3.1-10): 當 Node i 蒐集到所有 Evaluation 內的節點之認可印章後，便將資訊儲存至信任成員(TM)中，並利用 H_i 將 Node i 的識別號碼、公鑰、總信任值、過期時間算出雜湊值已證明資料未經修改。

(2) 信任證據互相驗證

為了要證實中央節點 Node i 的個別和總信任值是否正確，且要兼顧運算及頻寬的需求，本研究採用了區塊驗證的方式，即節點只向同一區塊驗證其信任值的方式。

由圖 28 可知 Node i 代表要被衡量的節點，它會以區塊(Block)的方式搜集各節點對它的個別衡量信任值，最後由 Node i 計算出總信任值，且做區塊驗證的動作，讓各區塊作個別的衡量。而衡量 Node i 的其他節點可稱之為 Node j，故可知為一對多的關係，即一個 Node i 節點對多個 Node j 節點。

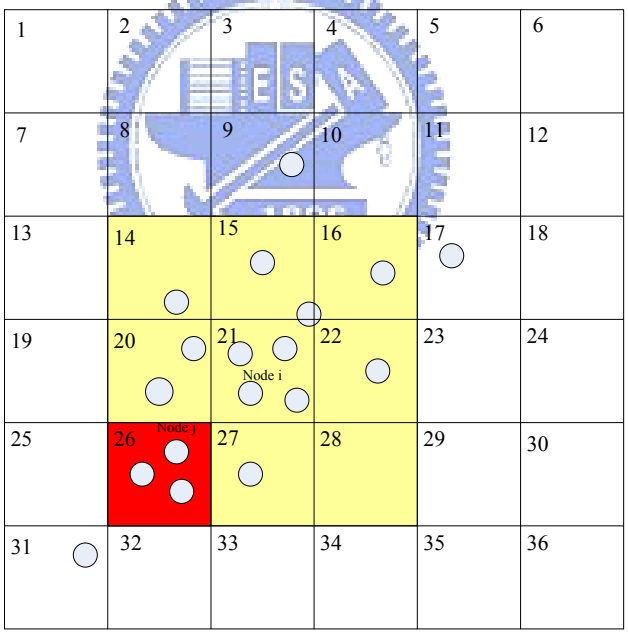


圖 28 區塊驗證圖

若求證通過，則會傳認可印章(Valid)回中央節點 Node i 表示驗證成功，如圖 29 所示。

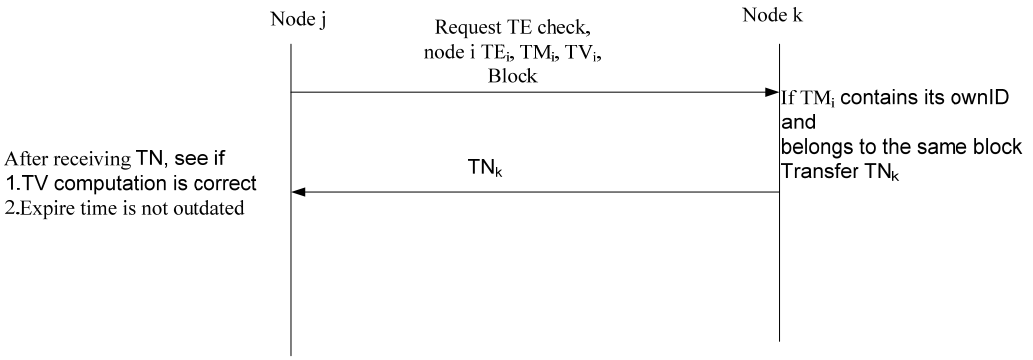


圖 29 區塊互相驗證流程圖

(3.2-1): 由 Node j 要求做信任證據互相驗證，並將 Node i 的信任證據、信任成員、總信任值，和 Node j 所在的區塊(Block)向四周廣播。

(3.2-2): Node k 收到廣播訊息後查看信任成員是否有它的識別號碼，若滿足條件且在同一區塊，則傳回它的信任節點(TN$_k$)。

(3.2-3): Node j 做以下動作

(a) 檢查 Node k 之信任節點(TN$_k$)的個別信任值是否和 Node i 之信任成員(TM$_i$)的個別信任值是否相同。

(b) 重算總信任值並比對是否相同。

(c) 衡量期間是否過期。

(3.2-4): 若滿足以上條件，則代表驗證成功，故可發送認可印章。

階段 4: 節點資料傳送時之個別信任值及總信任值的比較。

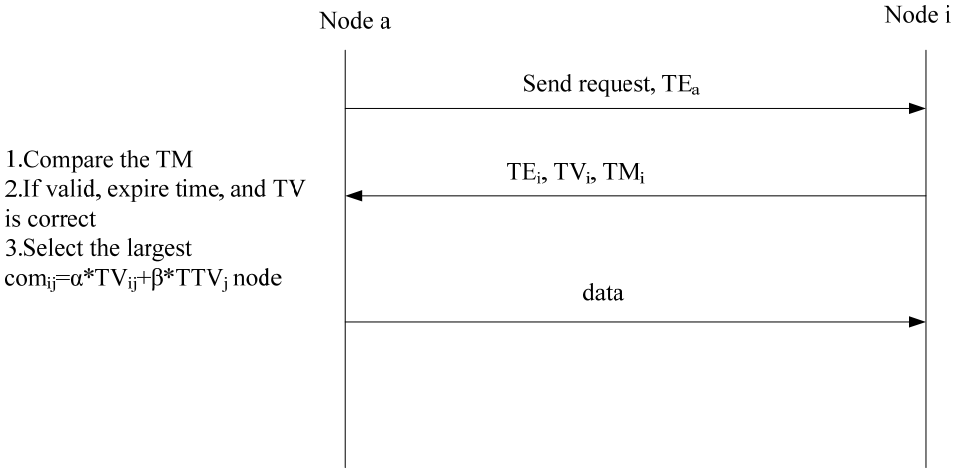


圖 30 節點資料傳送流程圖

(4-1): 當節點要求轉送資料時，會將它的轉送要求及信任證據傳送出去。

(4-2): 欲轉送節點將它的信任證據傳送。

(4-3): 節點比對

(a) 信任成員。

(b) 確認未過到期期限。

(c) 在傳送時分為兩種情況，第一種情況為傳送節點先前沒有跟中繼節點互動過，故會參考總信任值並選擇最高總信任值的節點傳送，即 com = TTV。第二種情況則是傳送節點先前有跟中繼節點互動過且得到了個別衡量值，所以可將個別信任值和總信任值依比例求出比較值(Compare)，即 com = α * TV + β * TTV，然後選擇最大比較值之節點請求傳輸，並增加此節點的個別衡量信任值。

然而當節點的總信任值低於最小可信任值(Minimun_trustworthy_value)，則代表節點因為其總信任值被評比太低導致於周圍節點認為它是一個永遠無法成為信任的節點，則永遠將此節點忽略而不會請求它傳送封包，然而此節點想要請求周圍節點代傳封包時，周圍節點永遠不會幫它轉送封包且不會和它合作。

(4-4): 傳送端將資料傳送，若中繼節點願意幫忙轉送封包，則傳送端會增加中繼節點的各別信任值作為補償，所以縱使中繼節點傳送封包需要耗費一定的電力，但是可藉由信任值的增加讓他在要求節點轉送封包時擁有優先被傳送的權利。

階段 5:節點離開行動無基礎網路。

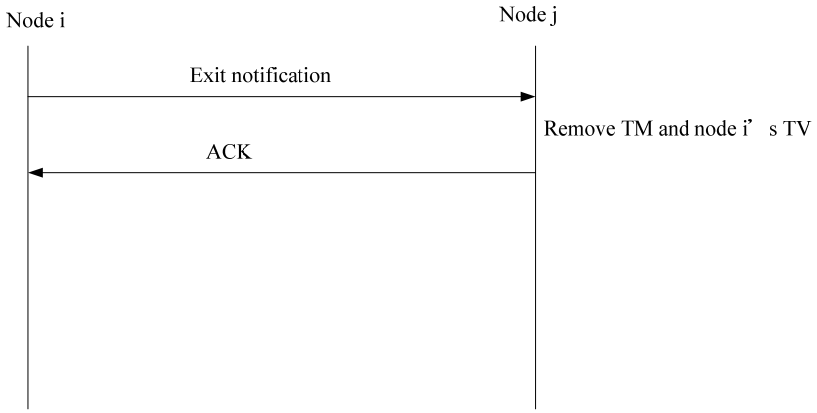


圖 31 節點離開之資料註銷流程圖

(5-1): 節點送出 Exit Notification 告知週遭節點離開訊息。

(5-2): 周圍節點將資料儲存並傳回 ACK，當下次節點登入時可以沿用先前的信任評比資料。倘若節點下次登入後其周圍節點先前沒有和它互動過，則可以藉由和其互動過的周圍節點取得此節點的信任值，並做為資料傳送的參考。

第四章 實作模擬與結果分析

4.1 模擬相關議題

4.1.1 模擬環境

本實驗會模擬信任證據在行動無基礎網路中的運作。當網路節點建構出行動無基礎網路環境時，節點會隨機的分佈並擁有一定範圍的傳輸信號能力，之後會依據實驗的參數下達而會有一定比例的隨機節點在隨機的時間變為自私節點或惡意節點。

在實驗所需的設備中，本實驗是以 IMB X31 的筆記型電腦作為實驗的硬體設備，而 CPU 是採用 Intel(R) Pentium(R) M processor 1500 MHz，並搭配 599MHz、256MB 的 RAM，作業系統是 Microsoft Windows XP Professional Version 2002。

為了驗證信任證據中所包含的各別信任值與經由散佈所算出的總信任值可以真正的反應在行動無基礎網路的節點信任狀況以及互動情況，本研究針對不同的網路環境中節點的互動情況，使用 NS2(Network Simulator Version 2)模擬套用信任證據的節點經由互動的情況。

NS2 是由柏克萊大學所開發的工具，以 OTcl 與 C++共同作為開發語言，使用者可藉由網路環境的建構並交由 NS2 模擬。因為 NS2 是開放原始碼(Open Source)的軟體，故可修改 NS2 內建的 C++函式庫，以模擬真實網路環境中節點互動的情況。

網路架構中包含了模擬路由器(Router)、鏈結(link)、網路節點(End Point)，模擬的網路介面(Network Interface)是採用無線網路作為信號傳輸的協定。佇列管理(Queue Management)是利用 DropTail 作為管理的方式，對每個佇列設置一個最大值，然後接受封包進入佇列，直到佇列長達到最大值，接下來到達的封包就會被拒絕進入佇列直到佇列的長度下降。繞徑則是使用 Distance Vector 的繞徑協

定，封包是利用 CBR(Constant Bit Rate)做傳輸，頻寬則是 2Mbps，並在 TCP 協定下使用 FTP 應用程式作傳送。

節點經互動後會有個別的信任衡量值 TV_{ij} 以及經計算後所得的 TTV_j。當節點要傳送資料時會依權重算出比較值 $com_{ij} = \alpha * TV_{ij} + \beta * TTV_j$，然後選擇比較值最大的節點請求傳送封包。在此實驗中會隨機指派節點成為惡意節點或自私節點，當節點背離時其信任值會降低，而節點合作後其信任值會增加，若總信任值低於最小可信任值則節點永遠被忽略，反之節點有改進之機會。

4.1.2 模擬參數

在考慮自私節點及惡意節點情況下，的模擬的時間是從 0 秒模擬至第 3.0 秒，故路由資訊仰賴鄰近節點所提供的資訊。本實驗會模擬在 5、10、15、20 個節點之下的傳送環境，並有 0%、20%、40%、60%、80%、100%自私節點或惡意節點的比例。

在尋找各別信任值與總信任值的比重時，會給予不同的權重比例，定義個別信任值的比重為 α、總信任值的比重為 β，其中 $0 \le \alpha \le 1$ 且 $0 \le \beta \le 1$，而 $\alpha + \beta = 1$。本實驗分別給予 $\alpha = 0.1$、$\beta = 0.9$; $\alpha = 0.25$、$\beta = 0.75$; $\alpha = 0.5$、$\beta = 0.5$; $\alpha = 0.9$、$\beta = 0.1$ 以模擬節點是否可以真正的反應真實的合作或背離情況。

4.1.3 模擬效率評估

為了評估實驗的結果，可模擬節點個數(Number of Nodes)、自私節點比例(Selfish Node Rate)、惡意節點比例(Malicious Node Rate)下沒有採用總信任值參考(Node Without Total Trust Value)以及採用總信任值參考(Node with Total Trust Value)下節點的互動情況。

根據互動結果，可利用三種效率評估的指標，第一個為平均End-to-End的時間延遲(Average End-to-End Delay Time, ADT)，計算封包由傳送端至接收端的時間並以秒作為計算單位，此評估標準主要是在衡量傳送端選擇中繼節點要求轉送封包後，其中繼節點是否為惡意節點以謊報假的路徑，讓封包傳遞時間比選擇其

他中繼節點還長。

- $ADT = \frac{\sum[end\_time(i) - start\_time(i)]}{number\_of\_packets}$

第二個效率評估指標則為平均產量(Average Throughput, ATP)，此指標評估節點效率的方式為單位時間內節點可處理的工作量，以Kbps為單位。

- $ATP = \frac{\sum packet\_byte(i) \times 8}{\sum[end\_time(i) - start\_time(i)] \times 1000}$

最後則為平均封包遺失率(Average Packet Loss Rate, APLR)，包含了傳送封包以及接收封包的數量，並算出封包遺失率，以比較當自私節點和惡意節點出現時，採取信任證據和無採取所造成的封包遺失率比較，且可在尋找個別信任值與總信任值的權重分配下，給予不同的權重時其封包遺失率比較。

- $APLR = \frac{\sum packet\_loss}{\sum packet\_sent}$

4.1.4 模擬案例

模擬案例(Simulation Case)分為三種狀況，在第一個案例為模擬於自私節點中，模擬採用總信任值與沒有採用總信任值節點傳送封包的情況。第二種案例則是在惡意節點的影響之下，節點會隨機的丟棄封包或者將封包路由至其他的節點，使得封包到達的時間延長，這時可比較有總信任值和沒有總信任值的情況下路由所受到的影響。

第三種案例假設行動無基礎網路中節點可任意的變成自私節點或惡意節點，因為周圍節點的評價可能會讓總信任值下降，直到比最小可信任值(Minimum_tustworthy_value)還低時，周圍節點會自動忽略此自私或惡意節點，所以為了避免成為被忽略的節點，中繼節點在背離之後會有一定的機率在往後的隨機時段改進成合作節點。而傳送節點在選擇中繼節點傳送時如果先前沒有和中繼節點互動過的話，則會參考總信任值(TTV)。又傳送端如果先前已經和中繼節點互動過的話，則會依各別信任值(TV)和總信任值的比例，即 com = α * TV + β *

TTV 選擇中繼節點傳輸。此實驗便代入不同的 α 與 β 的比例值以驗證何種比例最適合網路節點的選擇且最能反應信任的程度。

4.2 模擬流程

為了驗證信任證據於行動無基礎網路中可以達到節點的身分認證，並可透過參考信任值以及個別信任值選擇最合適節點要求轉送封包，本研究的模擬流程如下。

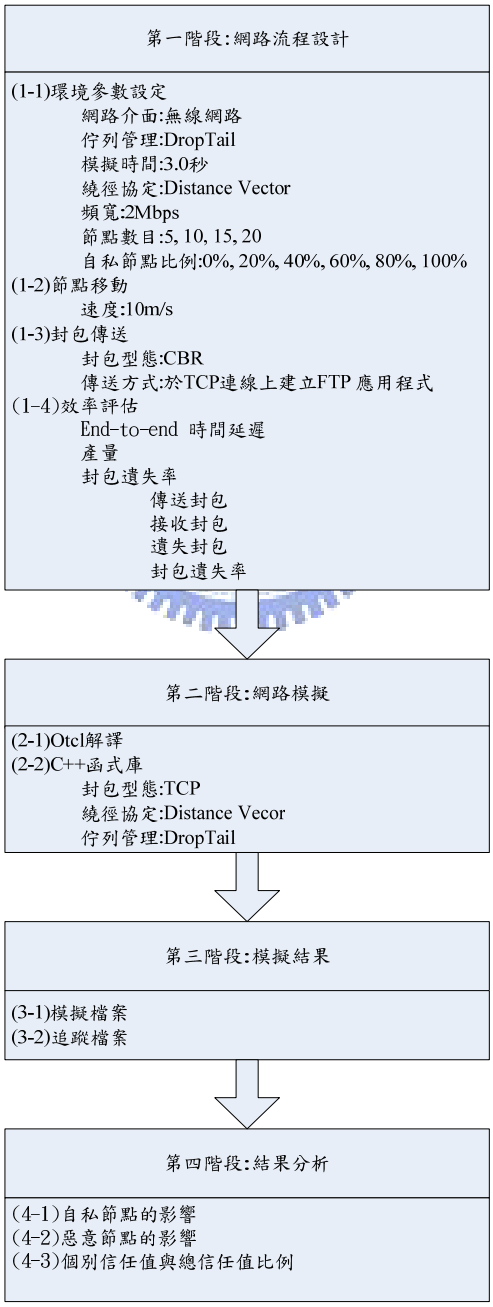


圖 32 模擬流程圖

階段 1:網路流程設計。

(1-1):環境參數設定

如4.1.2的參數環境設定。

(1-3):節點移動

節點移動的速度為10m/s。

(1-3):封包傳送

封包傳送的型態CBR(Constant Bit Rate)，當目的端收到封包後不須對封包的來源節點做回應。傳送方式則是在TCP連線上建立FTP應用程式傳輸。

(1-4):效率評估

評估 ADT、ATP、以及 APLR。

階段 2:網路模擬。

(2-1):OTcl解譯

OTcl解譯(OTcl Interpreter)會剖析網路情境並會是網路模擬的情況和C++函式庫進行功能的存取，然後在模擬結束後產生實驗結果的記錄檔，其中包含了out.nam以及out.tr檔案。

(2-2):C++函式庫

C++函式庫可供應不同的功能給OTcl使用，封包傳輸的型態為TCP、繞徑協定為Distance Vecor、佇列管理則是DropTail。

階段 3:模擬結果。

(3-1):模擬檔案

亦即out.nam，讓使用者透過模擬過程的播放了解其封包傳送的紀錄。

(3-2):追蹤檔案

利用awk程式語言所寫的記錄檔，可將out.tr透過awk來分析封包傳送後的資料。awk語言是使用直譯器(Interpreter)故不需先行編譯，其變數無型別之分，且awk可處理資料列以及欄位的資料，所以可以將模擬檔案的記錄檔擷取以做資料分析。

階段 4:模擬案例。

(4-1): 自私節點的影響

模擬自私節點的行為，此實驗模擬節點會將封包丟棄的狀況。

(4-2): 惡意節點的影響

針對Black Hole和Grey Hole問題，模擬封包被中繼節點隨機丟棄的情況，並將惡意回報路由路徑的狀況考慮。

(4-3): 個別信任值與總信任值比例

包含了傳送封包、接收封包、以及遺失封包的數量，並算出封包遺失率，以比較當自私節點和惡意節點出現時，採取信任證據和無採取所造成的封包遺失率比較，且可在尋找個別信任值與總信任值的權重分配下，不同的權重其封包遺失率比較。

4.3 案例一: 自私節點之總信任值參考比較

首先比較節點沒有總信任值與擁有總信任值的比較，因為節點在互動的過程中若周圍節點可以對中繼節點做出共同評價，所以當此中繼節點開始採取不合作的策略時，可優先被周圍節點偵測，並反應至總信任值中。所以傳送端可以馬上挑選其他的節點代為傳送。以下會針對節點有無參考總信任值的比較，本實驗會比較端點對端點的平均延遲時間(ADT)、平均產量(ATP)、以及平均封包遺失率(APLR)的不同，以證明提出之方法是有效的。

4.3.1 節點個數於自私節點之有無採用總信任值參考比較

首先比較封包由傳送端送出至接收端所經過的平均延遲時間。由圖 33 可知當節點數增加時，因為封包所傳送路徑變長且所通過的節點數增加，所以 ADT 會呈現增加的情況，中繼節點有隨機的機率在不定的時間變成自私節點，故會影響到封包的傳送。

當沒有採用總信任值參考的情況時，因為中繼節點背離，所以傳送端所傳的封包會被丟棄，等到節點發現沒有回傳 ACK 且想要利用 Distance Vector 協定找

尋其他節點傳送時已經過了一段時間，所以先前所傳的封包不但無法到達目的地，且會被自私節點丟棄。若採用總信任值參考，雖然中繼節點會於隨機時間背離，但是經由總信任值計算可以讓傳送節點在總信任值更新時盡快選擇第二順位之節點傳送封包。然而有參考總信任值的機制會比沒有參考總信任值機制之平均延遲時間會快 12.51%，雖然不是相當明顯，但仍然對封包的傳送速度有些許的提升。

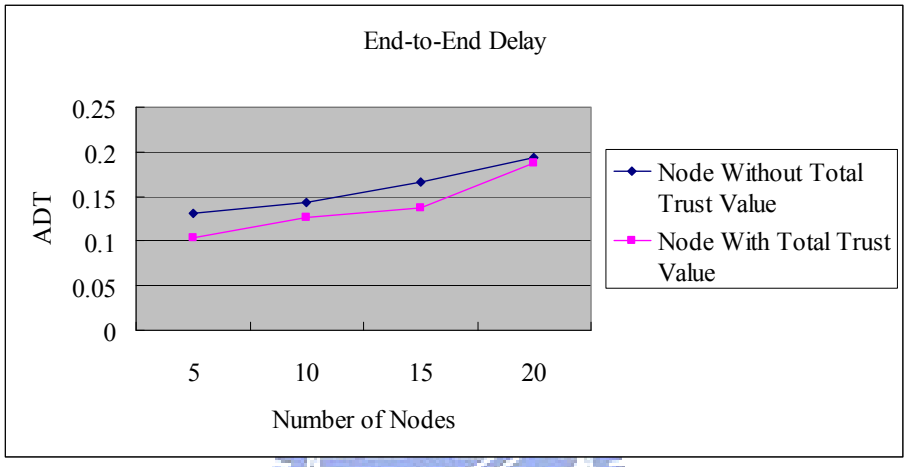


圖 33 自私節點有無總信任值參考 End-to-end 平均延遲時間比較

接下來比較有無總信任值參考之產量，圖 34 為有無總信任值參考之產量。當節點數增加時，因為封包路由所需經過的路徑及節點數增加，且可能因為自私節點的丟棄封包或封包錯誤的繞徑導致於 ATH 的降低。在沒有採用總信任值的參考時，因為中繼節點採取不合作的策略，且節點沒有及時的發現其行為，故所傳送的封包皆被丟棄，等到節點發現後利用 Distance Vector 協定找到第二條路徑時，其 ATH 才會穩定的上昇。整體在 ATH 中，有總信任值參考的產量會比無總信任值產量多 68.50%，這是因為本機制可以提早的將封包傳送至合作的節點，而不會被自私節點所拒絕傳送，故產量的增加較為明顯。

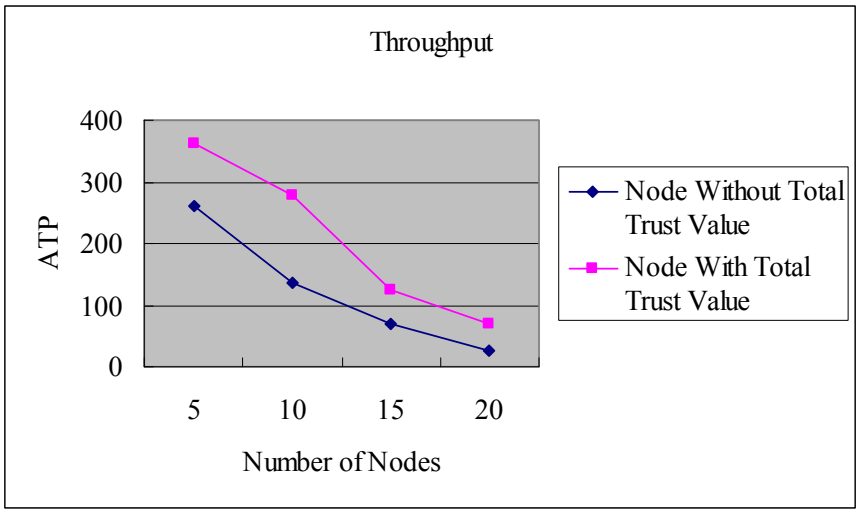


圖 34 自私節點有無總信任值參考平均產量比較

因為封包的路徑探索、自私節點的丟棄封包及其他因素會造成封包的遺失，當節點數增加時封包的遺失也會增加，所以需比較有參考總信任值的節點和無參考總信任值節點的封包遺失率。採取本研究的總信任參考機制時雖然起初傳送端節點傳封包至自私節點時封包會被丟棄，但是可以透過總信任值的參考了解其要求傳送的節點為自私節點，並可及時的找到其他中繼節點傳送資料，故只損失一小段時間的封包遺失。故由圖 35 可知有參考總信任值機制的 APLR 會比無參考總信任值低，且在節點為 10 個以上時其 APLR 會比無參考總信任值的為少的多。沒有採取參考機制會比採取總信任值參考機制之 APLR 會增加 18.71%，原因在於自私節點會將封包丟棄。

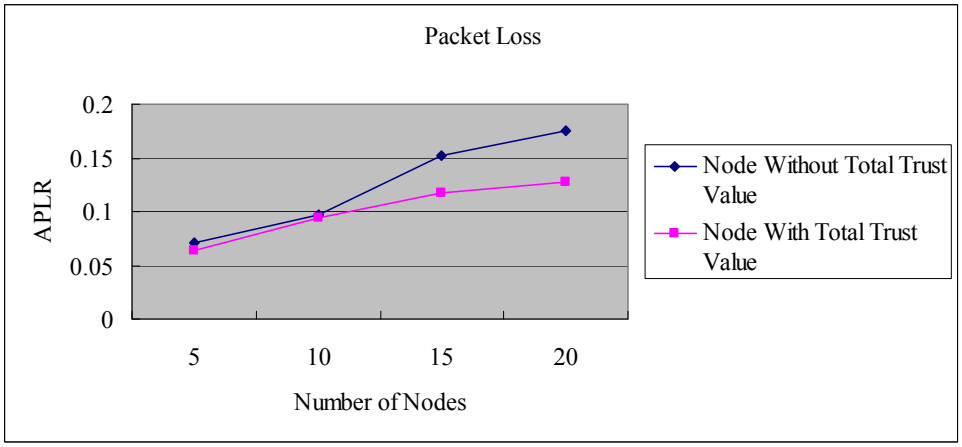


圖 35 自私節點有無總信任值參考平均封包遺失率比較

4.3.2 自私節點比例之有無採用總信任值參考比較

在比較完節點個數對自私節點的影響後，接下來評估網路節點中所包含的自私節點比例，實驗中會以隨機的方式在行動無基礎網路中選取一定機率的節點使之成為自私節點，這些節點也會以隨機的時間出現並將封包丟棄。此實驗會模擬在沒有自私節點或有 20%、40%、60%、80%、或全部節點皆為自私節點，以探討採用總信任值參考與平時的環境下的不同影響。

圖 36 為自私節點的比例對於 ADT 的比較，當網路中自私節點的比例增加時，代表有較多節點不採取合作的策略且會將封包丟棄。不過在採用總信任值時，傳送端節點可以及時的得到相關的路由資訊，避免將封包傳向自私節點，所以可得知參考總信任值的節點其 ADT 較無參考周圍節點評價的節點平均低了 25.32%。

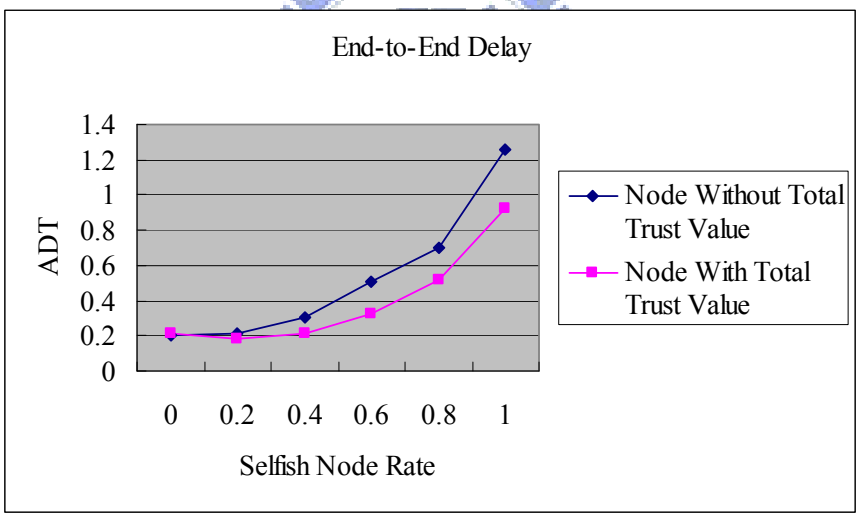


圖 36 自私節點比例之有無總信任值參考 End-to-End 平均延遲時間比較

圖 37 為不同比例的自私節點存在網路中的 ATH 比較，由此可知當網路沒有自私節點時，其 ATH 大約在 200kbps 左右，但是當網路存在 20%的自私節點時，其 ATH 會驟降至 50kbps，所以証明自私節點的存在會影響產量。有信任值參考節點之 ATH 會比沒有參考總信任值節點平均多 23.98%，其原因為當周圍節點意識到中繼節點為自私節點時，可調整其個別信任值，再經由信任值的散佈得到總信任值，讓傳送節點意識到自私節點的存在，故會避免將封包往自私節點傳送，

所以 ATH 會比沒有總信任值參考來的多。但是隨著自私節點比例增加，傳送節點逐漸無法選擇合作節點傳送，故其 ATH 的差異不會像 20%至 80%的比例那麼明顯。

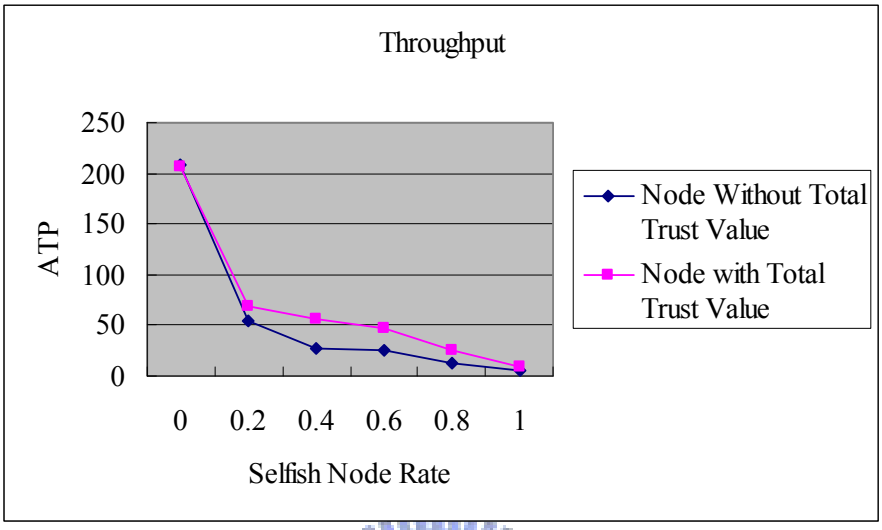


圖 37 自私節點比例之有無總信任值參考平均產量比較

最後比較 APLR，根據圖 37 可知雖然兩種機制皆會因為自私節點的比例增加而導致 APLR 的增加，但是採用總信任值參考節點其 APLR 會比沒有採用的低，且當自私節點比率越高時，其差距越明顯。而其 APLR 在採用總信任值的情況下會比沒有採用總信任值參考少 27.68%，故仍可以解決自私節點的問題。

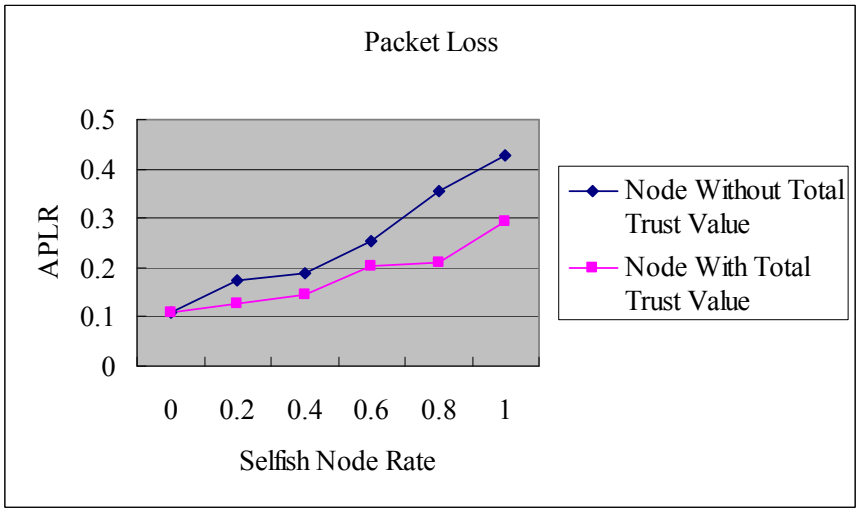


圖 38 自私節點比例之有無總信任值參考平均封包遺失率比較

此實作模擬著重於自私節點存在對封包傳送的影響，經由模擬可知有參考總

信任值機制其 ADT 在節點個數和自私節點比例會比無參考小 12.51%及 25.32%、ATH 會增加 68.50%及 23.98%、APLR 會減少 27.03%及 27.68%。故可證明由周圍節點所計算之參考總信任值可以讓傳送節點早一步轉換其他節點傳輸，且可避免中繼節點的背離所造成的傷害，所以可解決自私節點的問題。

本實驗均假設每一個節點都有餘力可傳送封包，但是實際上每個節點可能因為忙碌或環境關係無法傳送封包，而將封包暫時性的丟棄，這時若將其信任值降低則無法實際反應節點合作的情況。再者節點處於忙碌狀態及空閒狀態時幫忙傳送封包代表的意義不同，若於忙碌狀態時節點仍然傳送封包，則代表節點趨向於合作的意圖明顯，其信任值的評比增加幅度應該較空閒狀態節點為大。本實驗是基於節點皆處於空閒狀態的平等條件下探討合作與否的狀況，故無考慮其機會成本問題。

4.4 案例二: 惡意節點信任比較

惡意節點會透過不同的方式對封包造成程度不一的破壞及傷害，故此實驗會針對惡意節點的行為作模擬，中繼節點在封包傳輸至隨機時間會隨機將封包丟棄。本實驗模擬 Black Hole 以及 Grey Hole 的情況，以比較預設情況與採用總信任值參考兩種情況。

4.4.1 節點個數於惡意節點之有無採用總信任值參考比較

圖 39 為有無參考總信任值的 ADT 比較，因為封包有隨機的機率被丟棄，所以其 ADT 會呈現不穩定的狀態，且若封包遺失則不會有延遲時間的計算。在有參考總信任值時雖然因為節點的惡意遺棄封包，或給予錯誤的路由資訊而造成封包損失，但是經由總信任值的衡量可選擇另一條路徑傳送，故可避免繼續遺失封包。有參考信任值的延遲時間會比較短，這是因為節點會因為總信任值的告知及時的選擇備援的最佳路徑，所以 ADT 會較短。平均來說採用總信任值的節點其 ADT 會比無採用總信任值參考的 ADT 低 41.40%，原因在於惡意節點的假路由資訊會混淆 Distance Vector 的路由表格，讓傳送端節點傳送的封包到達接收端的

時間便長，若採用總信任值參考機制則可透過周圍節點的通報了解惡意節點的存在，避免將封包傳送到此節點。

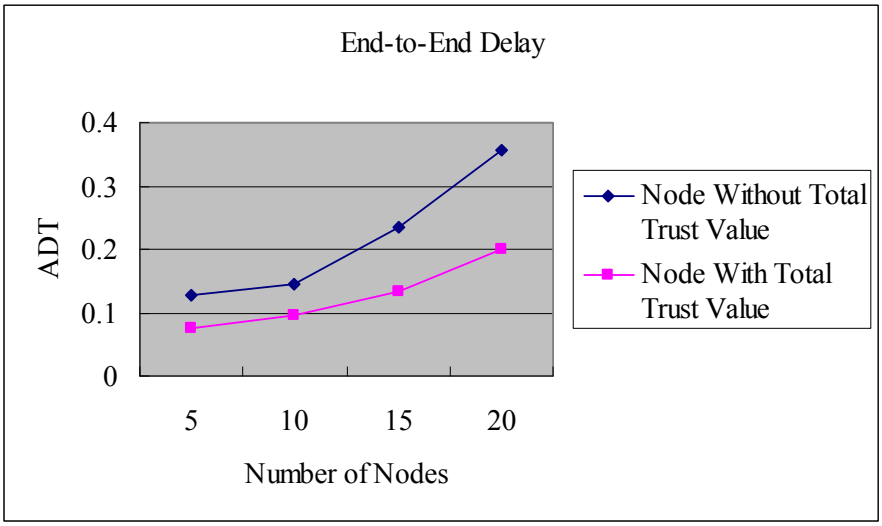


圖 39 惡意節點有無總信任值參考 End-to-end 平均延遲時間比較

接下來比較惡意節點對於產量的影響，圖 40 在沒有總信任值參考時，ATH 會呈現不穩定的情況，於 Distance Vector 的協定中，若封包丟棄至一定程度時便不會像此節點傳送封包，故 ATH 會較低。當有參考總信任值時，雖然先前會因為封包傳送而被惡意節點遺棄而產量會有斷斷續續的結果，但是藉由總信任值的反應可以及時的轉向另一節點，故 ATH 會比無總信任值參考高，其比例高達 114.12%，故此機制可明顯的解決惡意節點的問題。

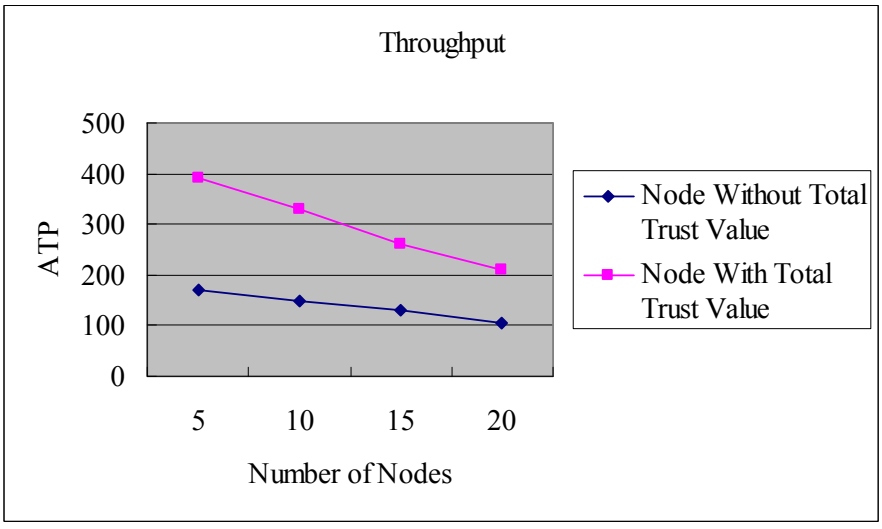


圖 40 惡意節點有無總信任值參考平均產量比較

圖 41 則是丟棄封包遺失比較，可知在節點數增加到 15 個以上時，其 APLR 會呈現激增的狀態，但是總體來說參考總信任值的封包遺失率會比較低。在沒有參考總信任值機制時其 APLR 比例會比參考總信任值高 39.75%，故此機制在封包遺失上也是可以明顯的解決惡意節點故意丟棄封包的問題。

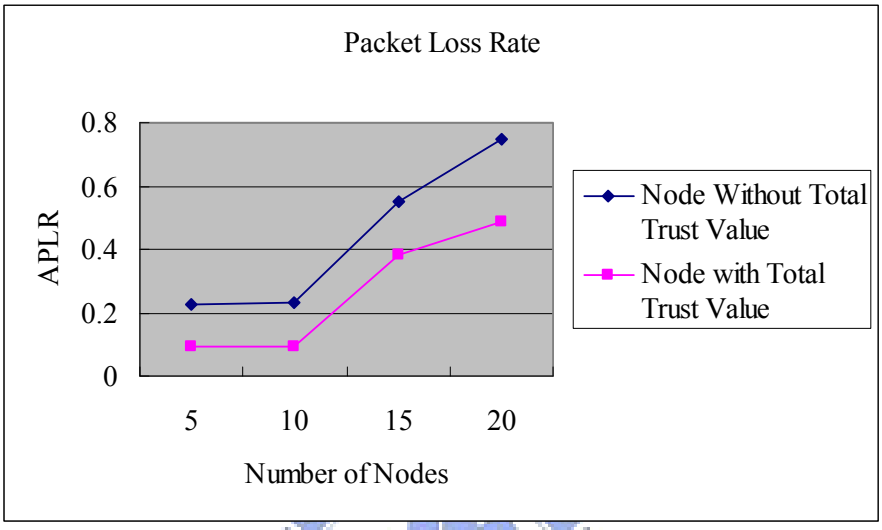


圖 41 惡意節點有無總信任值參考平均封包遺失率比較

4.4.2 惡意節點比例之有無採用總信任值參考比較

接下來討論有無導入總信任值參考的情況下，討論當網路上沒有惡意節點，乃至於有 20%、40%、60%、80%、與網路中全為惡意節點的績效評估。圖 42 說明當惡意節點的比例越高時，有導入總信任值參考機制的節點其 ADT 會比沒有導入的節點為快。有採用總信任值參考的節點於平均的 ADT 會比沒有採用的低 7.11%，故由此可知當惡意節點的比例越高時，封包的延遲亦會增加，而參考本機制之總信任值參考可讓封包到達接收端的時間縮短。但是隨著惡意節點的比例增加，其 ADT 會和無參考總信任值的相差無幾，因為周圍皆是惡意節點，故此機制適合在惡意節點比例較低的行動無基礎網路中運作。

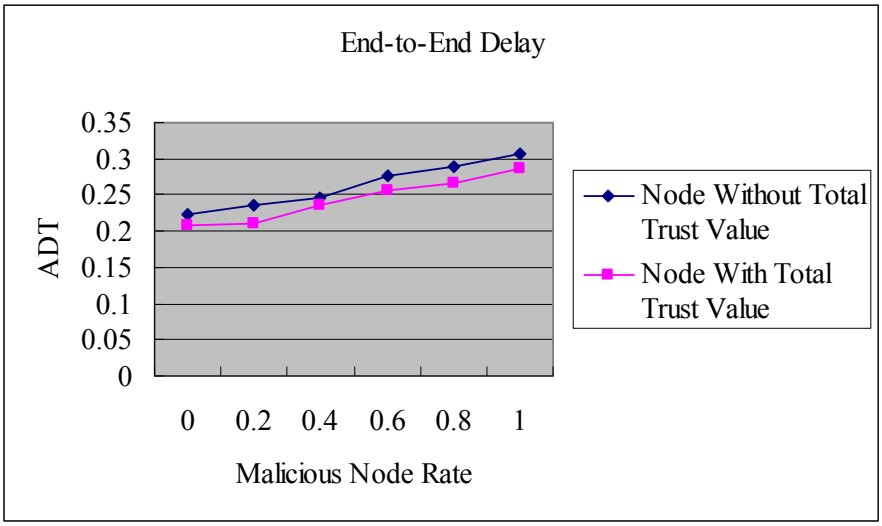


圖 42 惡意節點比例之有無總信任值參考 End-to-End 平均延遲時間比較

在 ATH 方面，由圖 43 可知當惡意節點的比例增加時，若沒有採用總信任值參考機制時，其 ATH 遞減的速度遠超過預期。然而周圍節點可以經由互動得知惡意節點為何，故降低它的總信任值，故其他節點就可避免傳送封包至此惡意節點，雖然因為節點數的增加也會導致 ATH 的減少，但是其減少的幅度比沒有採用總信任值參考的節點緩慢。其 AHT 比較中有採取總信任值參考機制平均會比沒有採用信任值參考多 92.92%，故可以讓平均封包處理量受到比較少的影響。

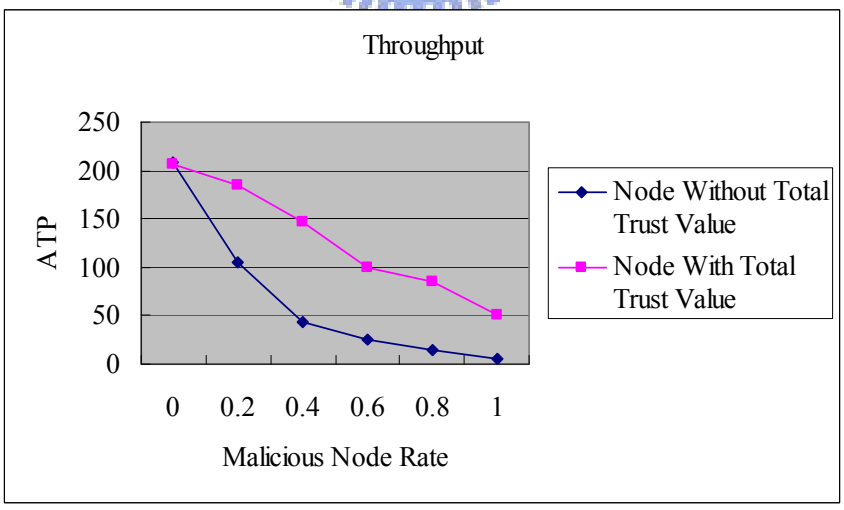


圖 43 惡意節點比例之有無總信任值參考平均產量比較

最後探討 APLR，如果沒有導入總信任值時，其 APLR 在惡意節點的比例增加時，會呈現激增的狀態，原因是惡意節點會假造路由資訊或傳送小部分的封

包，而傳送端會以為此節點是合作節點，故還是會傳封包給此節點，直到發現封包的 ACK 回傳過少並發現此節點原來是惡意節點時，也已經傳送了不少的封包出去。但是如果傳送端可以藉由總信任值的給予了解到此節點為惡意節點，故可避免將封包往此節點傳送，故 APLR 僅呈現緩慢的成長，其結果如圖 44 所示。然而採用本機制可以減少 62.76%的封包損失，故為較佳的方式。

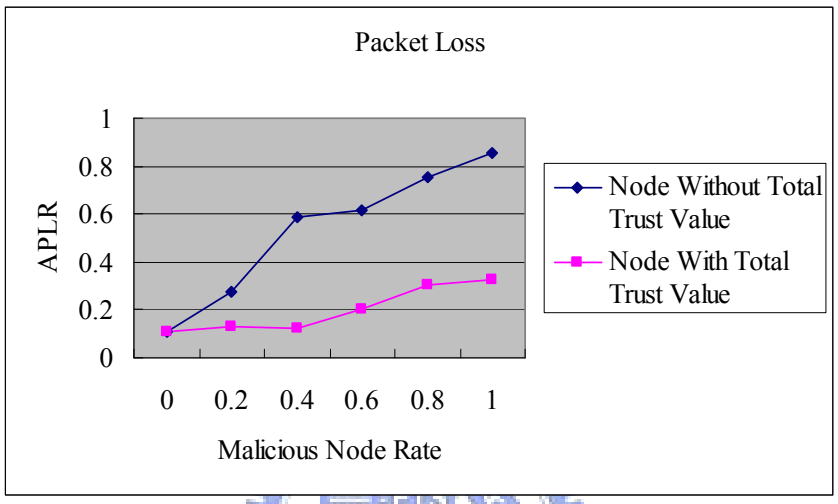


圖 44 惡意節點比例之有無總信任值參考平均封包遺失率比較

此機制可避免惡意節點的影響，藉由總信任值的調整，可搶先或及時的在惡意節點丟棄封包時，盡快選擇受信任的節點轉送封包，雖然路徑變長且延遲時間增加，但是可以避免封包被惡意遺棄所造成的損失。經由模擬可知有參考總信任值機制其 ATP 在節點個數和自私節點比例會比無參考小 41.40%及 7.11%、ATH 會增加 114.12%及 92.92%、APLR 會減少 27.03%及 62.76%，故與自私節點之模擬情境比較，經由信任散佈及總信任值計算可以顯著的解決惡意節點假造路由路徑以及丟棄一部份封包的策略。然而本實驗不考慮網路環境中因為頻寬及傳輸距離造成的封包丟棄情況，而假設封包皆可以到達周圍節點而不會被丟棄，以在環境條件相同的情況下探討惡意節點對網路的影響。又因為 Distance Vector 的特性使得節點數目過多，即路由表資訊無法儲存而造成無法決定路徑的情況，本實驗模擬 0 至 20 個節點存在對於網路的影響，以公平的比較有無採用本機制對於效率評估的影響。

4.5 案例三:個別信任值與總信任值權重分配

於信任證據建立後，可讓節點衡量周圍節點的信任程度，且周圍節點亦可計算此節點的信任值，經由信任證據的散佈讓節點將信任值整合計算得到總信任值。故在下一階段時節點當節點要傳送資料時，若先前傳送節點沒有和中繼節點互動過時，會以總信任值(TTV)作為比較值(com)。倘若傳送節點之前有和中繼節點互動過，則會依權重算出比較值 $com_{ij} = \alpha * TV_{ij} + \beta * TTV_j$，然後選擇比較值最大的節點請求傳送封包。

個別信任值的優點可以讓節點在總信任值更新之前讓個別節點測試中繼節點的信任程度，且適合傳送節點的做傳送封包狀態、頻寬測試、路徑選擇的環境測試，以得到適合路徑與中繼節點選擇情況。

然而若傳送節點沒有和中繼節點互動過，則可以利用周圍節點對此中繼節點的總信任值的參考來給予建議。如果傳送節點有和中繼節點互動過且得到各別信任值的衡量，但是傳送節點因為不同的因素導致於一段時間沒有再和此中繼節點互動，又在未來傳送節點想要重新找尋此中繼節點並想要請求傳送封包，而因為久未互動的關係傳送節點不知此中繼節點是否仍是合作節點，則亦可藉由總信任值的擷取得知此節點是否為合作節點。

為了找尋 α 與 β 值的比例，本實驗設計了中繼節點在不同的策略下，不同權重分配時所得到的結果模擬，以得到最佳的權重分配。此實驗會模擬節點會隨機背離，並在得知為有合作才會互相幫忙傳封包的情形下，在隨機時間改進並合作，故探討權重 α 與 β 在不同的情況下是否真實反應節點的背離及合作情況。

本實驗分別代入 $\alpha = 0.1$、$\beta = 0.9$; $\alpha = 0.25$、$\beta = 0.75$; $\alpha = 0.5$、$\beta = 0.5$; $\alpha = 0.9$、$\beta = 0.1$ 的權重，以算出傳送節點是否和中繼節點合作並傳送封包，總信任值會在隨機時間作更新。起初會給予隨機的節點數，中繼節點會有隨機的機率與隨機的時間成為自私節點或惡意節點，又會在隨機時間變為合作節點，以測試不同的權重下的封包 ADT、ATH、以及 APLR。

當各別信任值的比重過高時，因為在總信任值更新後無法適時反應出節點背離的情況，故還是往自私或惡意節點傳送封包，則所送的封包皆被丟棄。而總信任值的權重過高時，會導致在總信任值更新之前，若節點已經改過，而節點不會信任已經改進的中繼節點傳輸而還是往備援路徑傳輸，故其 ADT 會增加。

由圖 45 可知當 α = 0.25、β = 0.75 時，其 ADT 會最小，而當 α = 0.9、β = 0.1 時 ADT 最長。

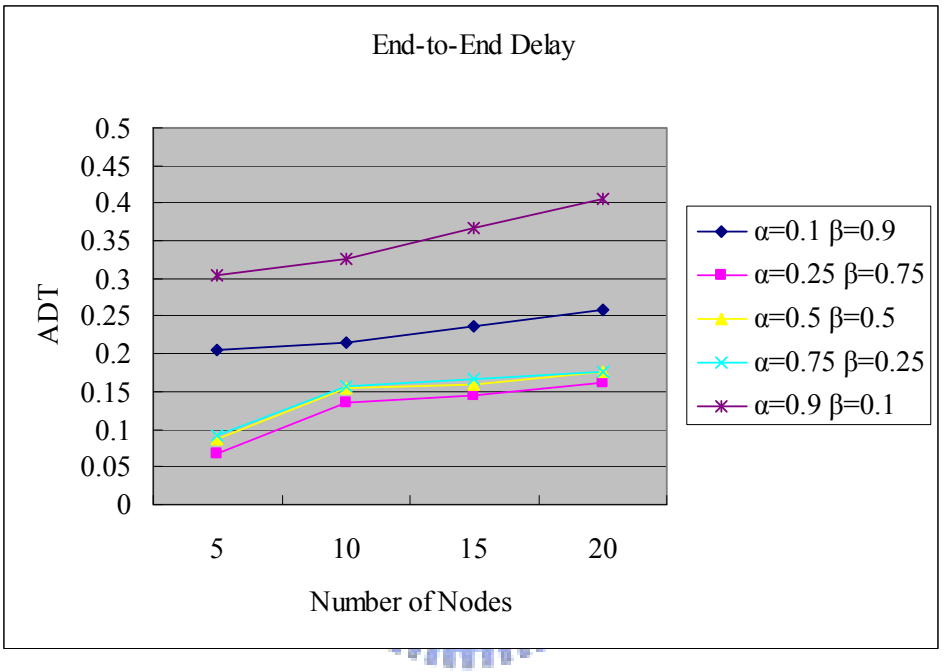


圖 45 個別信任值與總信任值權重分配 End-to-End 平均延遲時間

圖 46 可顯現出當 α = 0.25、β = 0.75 時其 ATH 為最高。

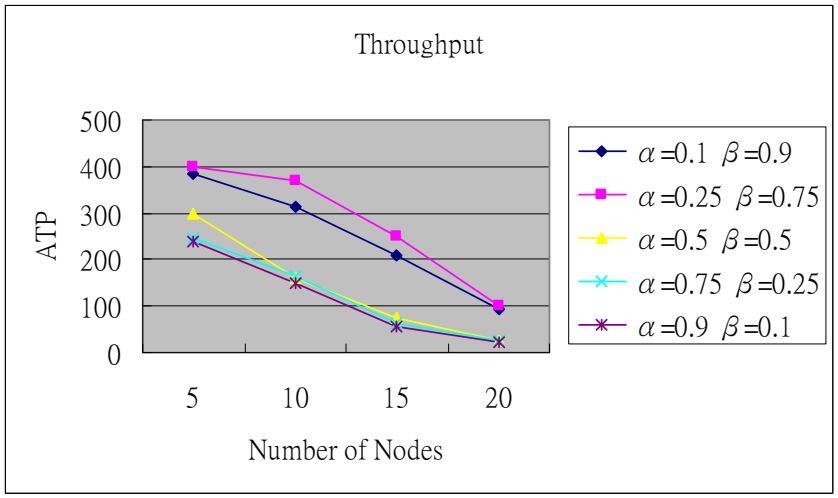


圖 46 個別信任值與總信任值權重分配平均產量

最後由圖 47 可知當 α＝0.25、β＝0.75 時其 APLR 也最小。

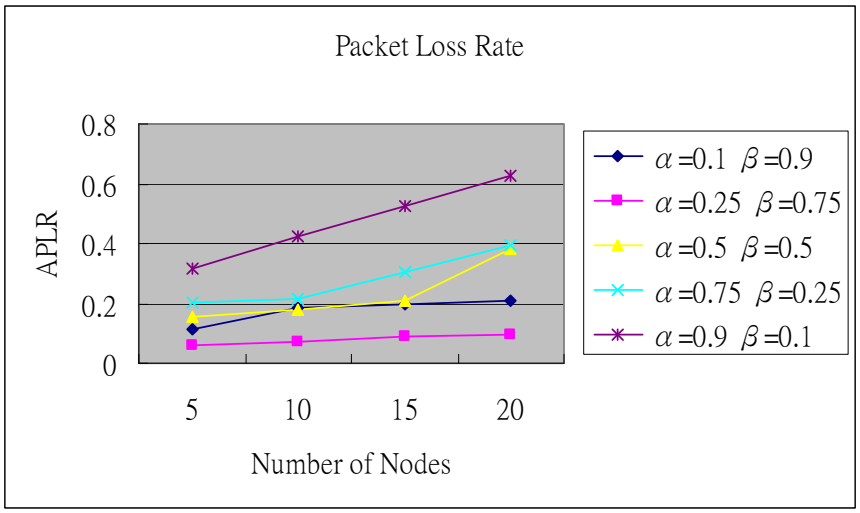


圖 47 個別信任值與總信任值權重分配平均封包遺失率

由以上的模擬可知，過大的各別信任值比重或過小的信任值比重對於行動無基礎網路中的節點的各別信任值與總信任值參考皆有不利的影響。當 α＝0.25、β＝0.75 時，其比重可以符合網路中在總信任值更新前與更新後的節點判斷。此實驗是代入五種權重比例制行動無基礎網路中以找出最適合行動無基礎網路的比重，而不是精確的算出何種比重最適合其環境，但是因為網路節點在每次實驗中所採取策略的時機以及決定是否合作的態度皆不同，故以等分比例的方式模擬環境以找出最適合的比重較為實際。

4.6 模擬結果比較

由上述的三種實驗，可知本研究所導入的各別信任值與總信任值參考可以解決自私節點與惡意節點的問題。然而當惡意節點的比例越高時，總信任值的參考可以避免傳送節點將封包傳至惡意節點，其時間延遲與封包遺失率的差距相當的明顯。輔助信任值的調整，讓中繼節點在耗費成本傳送封包時，可以藉由幫忙轉送封包得到好處，當下一次此節點想要請求其他節點幫忙傳送封包時，可以優先的幫它傳送，以獲得最大利益。表 11 針對自私節點與惡意節點中評估有導入總信任值參考與沒有導入總信任值參考中，其節點個數與自私或惡意節點比例所產生的 ADT、ATH、以及 APLR 比較，並列出改善前後所增進的比例，以證明本

機制可實際的於行動無基礎網路中解決自私點與惡意節點問題。

表 11 自私節點與惡意節點效率評估比較

Selfish Node		Node without TTV	Node with TTV	Improvement Ratio
Number of Nodes	ADT	0.1582	0.1384	12.51%
	ATR	123.602	208.2718	68.50%
	APLR	0.1239	0.1007	18.71%
Selfish Node Rate	ADT	0.5307	0.3963	25.32%
	ATR	55.5189	68.6832	23.98%
	APLR	0.2515	0.1819	27.68%
Malicious Node				
Number of Nodes	ADT	0.2160	0.1266	41.40%
	ATR	139.1408	297.9298	114.12%
	APLR	0.4386	0.2643	39.75%
Malicious Node Rate	ADT	0.2624	0.2437	7.11%
	ATR	67.1741	129.5934	92,92%
	APLR	0.5332	0.1986	62.76%

又為了找尋最適合的各別信任值與總信任值的比例，藉由模擬結果表 12 可知當 $\alpha = 0.25$、$\beta = 0.75$ 時可正確的判斷網路節點的行為，故可以在中繼節點背離時避免傳送封包，而當中繼節點開始採取合作態度時，也可以在第一時間與之合作

表 12 個別信任值與總信任值權重之效率評估比較

	ADT	ATR	APLR
$\alpha = 0.1$、$\beta = 0.9$	0.2281	250.2393	0.1764
$\alpha = 0.25$、$\beta = 0.75$	0.1279	280.3877	0.0796
$\alpha = 0.5$、$\beta = 0.5$	0.1438	139.9456	0.2315
$\alpha = 0.75$、$\beta = 0.25$	0.1478	124.8181	0.2797
$\alpha = 0.9$、$\beta = 0.1$	0.3508	116.0667	0.4727

第五章 行動無基礎網路信任賽局分析

網路節點會根據行動無基礎網路中的信任狀況而導致不同的策略採行，最終有不同的互動結果。本研究針對信任證據通訊與信任值計算機制中，階段 4 探討當節點要選擇中繼節點傳送封包或被請求傳送封包時，為了保證節點可以因為合作而獲得最大的利益，可利用賽局分析其行為，並用標準式賽局量化表示其行動所得的結果組合及相對應的報酬，讓合作的節點可以於行動無基礎網路中擁有優先的封包傳送權利，且使得不合作的自私節點以及惡意節點自動被網路所忽略。為了讓節點合作，當節點背離(Deviate)而使得信任值降低至最小可信任值時，網路節點將永遠不會信任此節點，所以節點會為了請求周圍節點幫忙轉送封包而會採取合作的策略。

5.1 賽局符號定義

在進行賽局分析之前，需要定義賽局分析所需要的參數，其整理如下。

- n_1: 封包傳送端節點，節點可以發出要求封包傳送訊息，以獲得中繼節點的總信任值(TTV)。若先前沒有和其中繼節點互動，則比較值為 com = TTV。若先前有互動過則比較值為 com = α * TV + β * TTV。最後選擇比較值最大的節點傳送封包以尋求接力傳至接收端。
- n_2: 於連續傳送封包賽局中為中繼節點以轉送封包，傳送節點 n_1 會依據比較值選擇最受信任的節點，其中繼節點可以選擇幫忙轉送封包或丟棄封包。而在想互傳送封包賽局中 n_2 可為傳送節點，也可當作中繼節點。
- d: 為接收端節點，n_1 會請求中繼節點以接力傳輸的方式將封包傳送至目的接收節點。
- r_i: 備援節點 i。當被選擇的中繼節點 n_2 若選擇不合作的策略而將封包丟棄，則 n_1 會依據比較值選擇其他節點傳送，其第一個被選擇做備援節點為 r_i ，以此類推至周圍無備援節點為止。
- R(Reward): 當雙方合作時，因為傳送封包而獲得的個別信任值增加，而會收

到的利益。

- C(Cost): 傳送封包所要耗費的成本，例如電力。
- S_i: 當 n_2 背離而不轉送封包時，定義 n_1 找尋其他備援節點 r_i 代傳所需要的獎賞為 S_i。
- Payoff: 節點互動後定義總共會獲得的報酬。節點傳送封包後會給予一定的信任值增加，故會得到獎賞，但是傳送封包會失去一定的成本，若節點合作則定義節點會得到 R-C 的報酬，如果選擇備援節點則會得到 S-C 的報酬。
- Θ_j(Extra Benefit): 為惡意節點 j 背離後所獲得的額外報酬，其報酬會比合作所得的 R-C 還大，但是在下一階段周圍節點不會信任此節點。
- p_i: 為備援節點 r_i 願意去轉送封包的機率。
- q_i: 為找到備援節點 r_i 的機率。

5.2 賽局評估效用分析

在分析賽局互動的情況中，可以算出當節點合作後所持續的長期合作報酬，以及一方節點背離後，兩者所產生的短期合作報酬。為了證明經由長期合作後所產生的報酬可以大於短期合作報酬，以使得節點會趨向合作以獲得最大的利益，本研究會分析在連續封包傳送以及相互封包傳送的賽局。又因為本研究有導入總信任值參考，故可以藉由個別信任值和總信任值的比重加總得到中繼節點的比較值，故當最大比較值的節點背離後，可以即時選擇備援節點傳送，讓損失減到最低的程度。

- 長期合作報酬(Long-Term Payoff, LTP): 由於節點合作會使得報酬增加，故定義經由合作階段後報酬的累計為長期合作報酬。
- 短期合作報酬(Short-Term Payoff, STP): 在互動至一定的階段後，節點背離至一定的程度而使得其總信任值(TTV)低於最小可信任值(Minimun_Trustworthy_Value)，而導致於行動無基礎網路節點永遠不信任其節點，則經由先前所合作的報酬再加上背離後的報酬稱為短期合作報酬。

為了證明合作後得到的長期合作報酬累計會大於背離後得到的暫時報酬，故需假設 X 為中繼節點在第 X 階段採取不合作的行動後，其總信任值小於最小可信任值，故此節點會永遠被周圍節點所忽略。而因為當節點合作後，於往後階段都會一直採取信任的策略，所以其 R-C 的小額報酬會一直累加，故假設 Y 為在合作的狀態下，在第 Y 階段時合作所累計的報酬會大於第 X 階段的報酬，其表示圖如 48 所示。

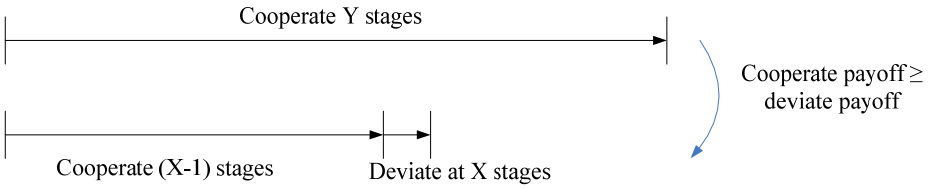


圖 48 合作報酬大於背離報酬表示

5.3 信任賽局之連續封包傳送問題

先前的文獻[18]已討論節點在行動無基礎網路中節點可能遇到的問題，本節討論在實作本研究所提出的信任證據中，其個別信任值與總信任值在社會網路中的運作。於連續封包傳輸時，可由圖 49 表示其節點連續傳送問題的情況。

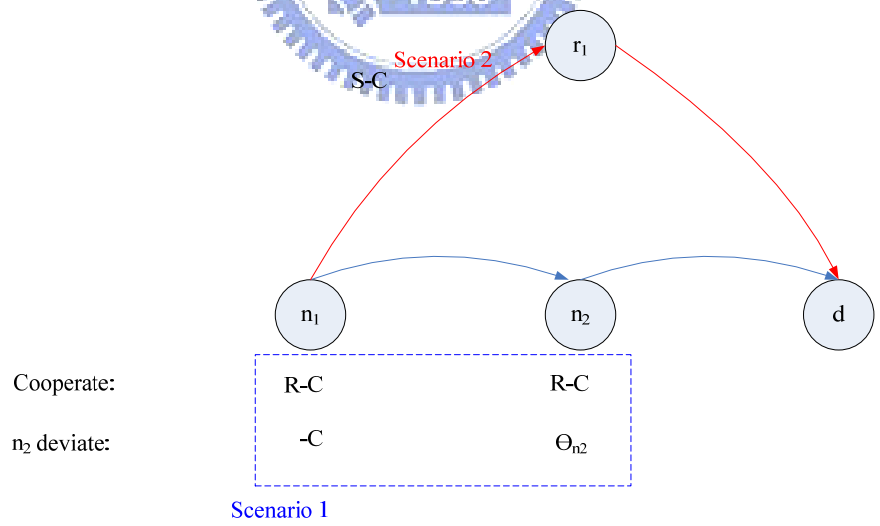


圖 49 信任賽局之連續封包傳送問題

傳送端 n_1 由會經由個別信任值與總信任值的權重分配找尋適合的節點代傳封包至最終接收節點 d。圖 49 可分為兩種情況，在第一種情況時若 n_2 採取合作的策略則雙方會各得到 R-C 的報酬，賽局互動也會持續進行。如果 n_2 採取不合

作的策略，則 n_1 不但無法將封包傳送至接收端，而且會耗費將封包傳往 n_2 節點的成本 C，不僅如此，還要進入第二階段繼續的尋找替代節點 r_1 以幫忙轉送封包，而可以因為這次的背離而得到額外的利益 Θn_2。故在第二階段時 n_1 會找尋 r_1 來轉送封包，若答應幫忙轉送封包時雙方會各得到 S-C，若 r_1 也背離合作的關係而不轉送封包時，又會浪費成本 C 且 n_1 無法將封包傳往目的地，而 r_1 會得到額外的利益 Θr_1。

5.2.1 連續封包傳送擴展式賽局

圖 50 以一階段連續封包傳送擴展式賽局之樹狀圖表示連續封包傳送的第一種情況，當兩節點皆傳送封包時可以各自得到 R-C 的報酬，當 n_2 背離時 n_1 無法將封包傳往目的地，若 n_1 沒有傳送封包時因為 n_2 也無法對封包做處理，所以皆無得到任何的報酬。

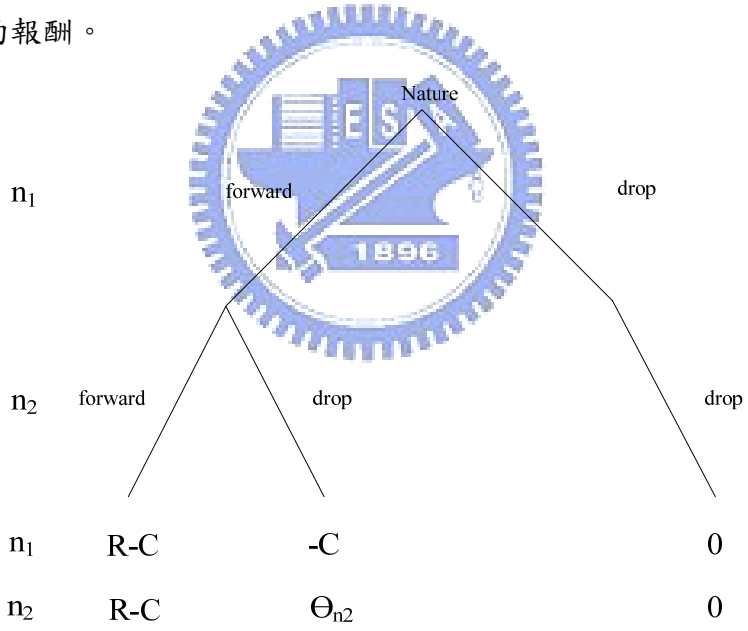


圖 50 狀況一:一階段連續封包傳送擴展式賽局

圖 51 則是當 n_1 無法透過最適合節點傳送封包時，需找尋備援節點的一階段連續封包傳送擴展式賽局。若 n_1 找到此 r_1 備用節點且 r_1 願意轉送封包時，兩者會各得到 S-C 的報酬，反之若 r_1 也無法傳送封包時，r_1 亦會得到 Θr_1，而 n_1 也浪費了成本 C 去轉送封包。同樣的如果 n_1 沒有將封包試著傳往 r_1 時，r_1 也是無法做任何決策。

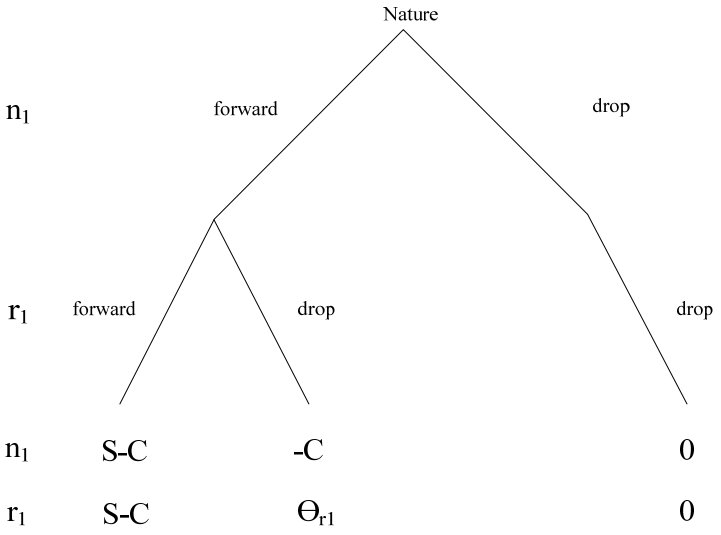


圖 51 狀況二:一階段連續封包傳送擴展式賽局

5.2.2 連續封包傳送標準形式賽局

根據以上的擴展形式賽局，可以整理成表的連續封包標準形式賽局，所以表 13 為第一階段的 n_1 和 n_2 互動結果表示結果組合。

表 13 第一階段連續封包傳送問題標準形式賽局

n_1 \ n_2	Forward	Drop
Forward	R-C, R-C	-C, Θ_{n2} Find r1
Drop	0, 0	0, 0

若 n_2 背離，則可進入第二階段，其組合如表 14 所示。

表 14 第二階段連續封包傳送問題標準形式賽局

n_1 or n_2 \ r_1	Forward	Drop
Forward	S-C, S-C	-C, Θ_{r1}
Drop	0, 0	0, 0

綜合表 13 及表 14 的第一及第二階段的標準形式賽局，可得到 n_1 和其他節點互動的連續封包傳送標準形式賽局，由表 15 可知若 n_2 不與 n_1 合作時會尋求和

備用節點 r_1 合作，如果 r_1 也不合作時此賽局也會中止，且 n_1 亦無法將封包傳往目的地。反之 n_1 可以透過節點將封包傳給目的節點並完成任務。

表 15 連續封包傳送標準形式賽局

		n_2		r_1	
		Forward	Drop	Forward	Drop
n_1	Forward	R-C, R-C	-C, Θ_{n2}	S-C, S-C	-C, Θ_{r1}
	Drop	0, 0	0, 0	0, 0	0, 0

表 16 將上述節點所採取的行動後，會得到的報酬整理成連續封包傳送總報酬表，故可知在行動中當節點合作時，n_1 和 n_2 都會得到 R-C 的總報酬。然而當 n_2 背離後，如果 n_1 找的到第三方 r_1 轉送封包時，n_1 會得到 S-2C 的總報酬;而若 r_1 也不幫忙轉送封包時，會損失 2C 且無法將封包傳向目的節點。

表 16 連續封包傳送總報酬

Players / Actions		n_1	n_2	r_1
Cooperate		R-C	R-C	0
n_2 deviates	r_1 forward	S-2C	Θ_{n2}	S-C
	r_1 drop	-2C	Θ_{n2}	Θ_{r1}

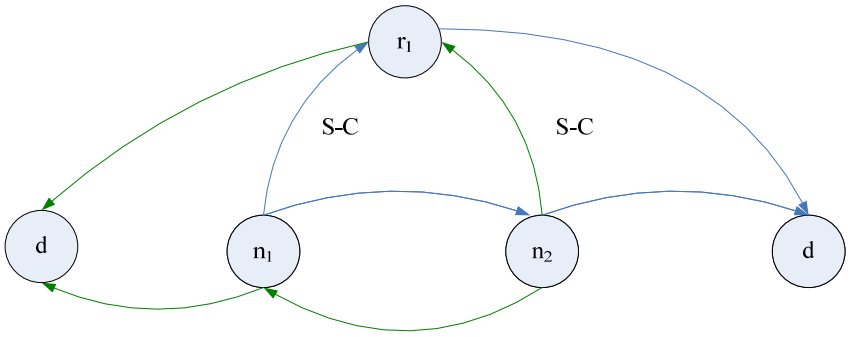
對於 n_1 來說，當 n_1 與 n_2 合作時，其 R-C 之報酬會因為往後階段的互動而累計，其合作報酬為 LTP = Y(R-C)。而 n_2 因為背離而導致 n_1 永遠不信任 n_2 時，因為在(X-1)階段雙方合作，所以會得到(X-1)(R-C)的報酬。但是在第 X 階段 n_1 永遠不信任 n_2，則 n_1 會浪費傳往的成本 C，再加上請求第三方轉送的報酬 p(S-C)+(1-p)(-C)，所以 n_1 的總報酬為 STP = (X-1)(R-C)-C+ p(S-C)+(1-p)(-C)。所以經由長期合作報酬累計大於短期背離的總報酬的法則得知 LTP ≥ STP，即 Y(R-C) ≥ (X-1)(R-C)+ pS-2C。

以 n_2 的角度觀之，若採取合作的策略，則也會得到 LTP = Y(R-C)的總報酬。倘若 n_2 決定背離且其信任值低於最小可信任值且使得週圍節點皆永不信任 n_2 時，雖然會得到短期的 Θ_{n2} 值且有總報酬 STP = (X-1)(R-C)+ Θ_{n2}，但是經由長期合作報酬累計大於短期背離的總報酬的法則，可以推得當 LTP ≥ STP 即 Y(R-C) ≥ (X-1)(R-C)+ Θ_{n2} 時，會趨向於合作以獲得最大的長期報酬。

5.4 信任賽局之相互封包傳送問題

在探討完單一方向的連續封包傳送問題後，可進一步的分析相互傳送封包問題，因為在連續封包傳送問題中，傳送端會傾向於合作，但是因為中繼節點不會請求傳送端幫忙傳送封包，故會有背離的可能性。於信任賽局之相互封包傳送中，節點皆有可能傳送或被周圍節點請求轉送封包，故它與周圍節點的互動結果會反應至下一階段的封包選擇傳送。如果節點背離至某一程度而導致此惡意或自私節點永遠被忽略，則其損失不只於短暫背離所失去的報酬，也包含了下一階段當它需要周圍節點傳送時，周圍節點永遠不會幫它傳送的懲罰。

由圖 52 可知當 n_1 及 n_2 節點合作時，兩者會各收到 R 的利益，但是傳送封包需要耗費一定的成本 C，所以兩者會得到 R-C 的報酬。如果有一方背離的話，則此方會得到額外的報酬 Θ;而被背離方則需要找尋網路中的其他周圍節點 r_1 來請求傳送封包，故會得到 S-C。



Cooperate:	R-C	R-C
n_1 deviate:	Θ_{n1}	-C
n_2 deviate:	-C	Θ_{n2}

圖 52 相互封包傳送問題

5.4.1 相互封包傳送擴展式賽局

由示意圖 52 可推導出兩階段擴展式賽局，n_1 和 n_2 合作的話會各得到 R-C 之報酬，然而如果有一方背離，則此方會得到相關的 Θ，但是另一方永遠不會和此節點合作，故此節點往後不會被請求傳送封包，相對的當此節點要求周圍節點傳送封包時，周圍節點也不會幫助此惡意節點傳送封包，所以此節點會被行動無基礎網路中的節點所忽略。要求傳送封包的原節點因為無法第一時間傳送封包至目的地 d，所以會找尋周圍節點 r_1 來轉送封包，故會跳至第二階段，如表示如圖 53 所示。

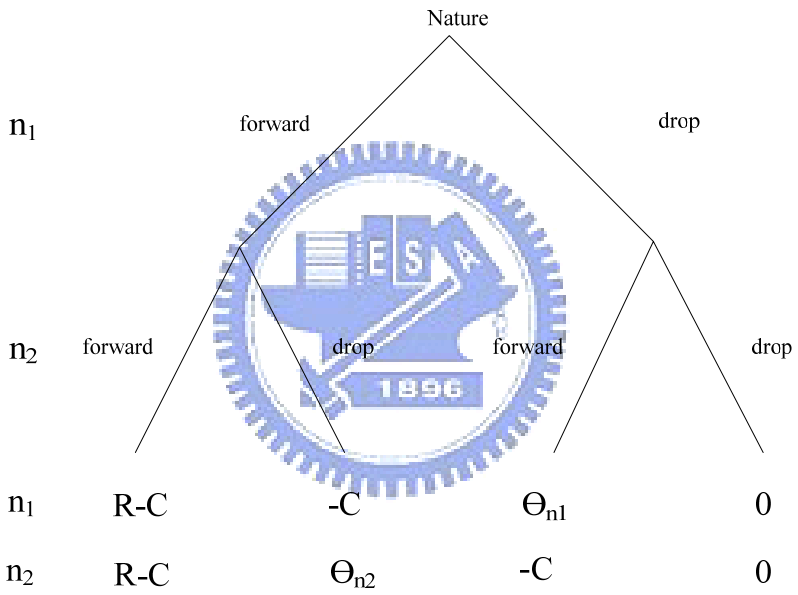


圖 53 狀況一:一階段相互封包傳送擴展式賽局

在第二階段中，原節點會和 r_1 做連續封包傳送的互動，若 r_1 答應幫忙轉送封包，則雙方會各得到 S-C 的報酬，如果 r_1 決定採取背離的策略，則 n_1 和 n_2 又會損失成本 C，且無法將封包傳送至目的地。

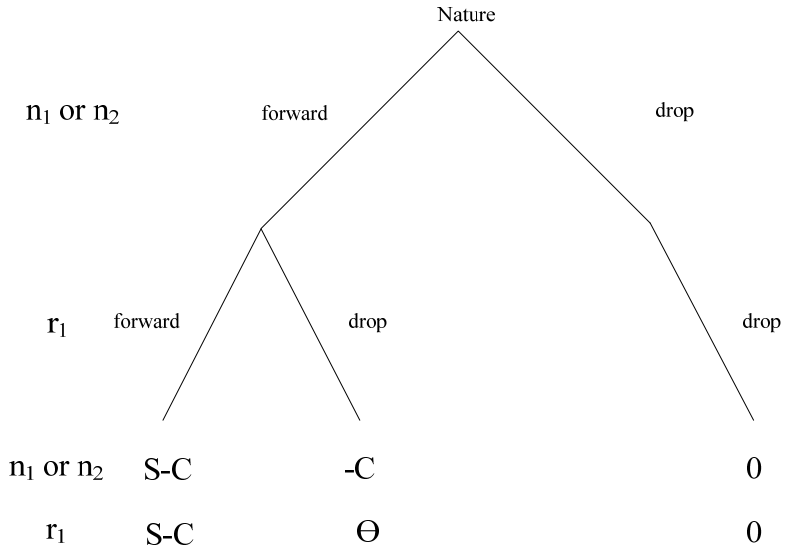


圖 54 狀況二:一階段相互封包傳送擴展式賽局

5.4.2 相互封包傳送標準形式賽局

表 17 以表格的方式呈現第一階段標準形式賽局。故可知若節點 n_1 和 n_2 若有一方背離時，背離方會得到相對的 Θ 值，而另一方就必須進入第二階段去尋找第三方 r_1 去請求轉送封包。

表 17 第一階段相互封包傳送問題標準形式賽局

n_1 \ n_2	Forward	Drop
Forward	R-C, R-C	-C, Θ_{n2} Find r1
Drop	Θ_{n1}, -C Find r_1	0, 0

當 n_1 或 n_2 因為另一方的背離而找尋 r_1 節點採取行動後所得到的報酬如表 18 所示，故和連續封包傳送問題相同。

表 18 第二階段相互封包傳送問題標準形式賽局

n_1 or n_2 \ r_1	Forward	Drop
Forward	S-C, S-C	-C, Θ_{r1}
Drop	0, 0	0, 0

整合表 17 和表 18 的相互封包傳送問題標準形式賽局，可得到表 19 的節點互動相互封包傳送標準形式賽局。當 n_2 不與 n_1 合作時，n_2 會得到短暫的報酬 Θ_{n2}，而 n_1 則會尋求和備用節點 r_1 合作，如果 r_1 也不合作時此賽局也會中止，且 n_1 亦無法將封包傳往目的地，反之 n_1 可以透過節點將封包傳給目的節點並完成任務。相對的如果 n_1 決定背離時，他也會得到短暫的報酬 Θ_{n1}，且要找尋第三方節點代傳封包。同理 n_2 也會有相互對應的情況，故不加以詳述。

表 19 相互封包傳送標準形式賽局

		N_1		n_2		r_1	
		Forward	Drop	Forward	Drop	Forward	Drop
n_1	Forward	0, 0	0, 0	R-C, R-C	-C, Θ_{n2}	S-C, S-C	-C, Θ_{r1}
	Drop	0, 0	0, 0	Θ_{n1}, -C	0, 0	0, 0	0, 0
n_2	Forward	R-C, R-C	-C, Θ_{n1}	0, 0	0, 0	S-C, S-C	-C, Θ_{r1}
	Drop	Θ_{n2}, -C	0, 0	0, 0	0, 0	0, 0	0, 0

表 20 將上述節點所採取的行動後，會得到的報酬整理成相互封包傳送總報酬表，故可知在行動中當節點合作時，n_1 和 n_2 都會得到 R-C 的總報酬。然而當 n_2 一方背離後，如果另一方能找的到第三方 r_1 轉送封包時，會得到 S-2C 的總報酬，而第三方節點 r_1 會得到 S-C 的報酬;而若 r_1 也不幫忙轉送封包時，則傳送端會損失 2C 且無法將封包傳向目的節點。

表 20 相互封包傳送總報酬

Actions \ Players		n_1	n_2	r_1
Cooperate		R-C	R-C	0
n_2 deviates	r_1 forward	S-2C	Θ_{n2}	S-C
	r_1 drop	-2C	Θ_{n2}	Θ_{r1}
n_1 deviates	r_1 forward	Θ_{n1}	S-2C	S-C
	r_1 drop	Θ_{n1}	-2C	Θ_{r1}

對於 n_1 來說，當 n_1 與 n_2 合作時，其合作報酬為 LTP = Y(R-C)。而當 n_2 因為背離而導致 n_1 永遠不信任 n_2 時，會得到 STP = (X-1)(R-C)+ pS-2C 的報酬。又如果 n_1 背離時，會得到暫時性報酬 STP = (X-1)(R-C)+ Θ_{n1}，為了要滿足長期合作報酬累計大於短期背離的總報酬，所以可以綜何以上的推論，確定當以下的兩個條件符合時，n_1 及 n_2 會尋求合作以獲取最大的報酬並在行動無基礎網路中生存。

推論 1:

LTP = Y(R-C) ≥ STP = (X-1)(R-C)+ pS-2C，當 n_2 背離。

LTP = Y(R-C) ≥ STP = (X-1)(R-C)+ Θ_{n1}，當 n_1 背離。

對於 n_2 來說，其推論和 n_1 相類似，亦可得到近似的推論。

推論 2:

LTP = Y(R-C) ≥ STP = (X-1)(R-C)+ pS-2C，當 n_1 背離。

LTP = Y(R-C) ≥ STP = (X-1)(R-C)+ Θ_{n2}，當 n_2 背離。

所以當推論 1 及 2 成立時，可以證明網路節點為了在行動無基礎網路中以信任的節點狀態存在以獲取長期的報酬，其必須配合轉送封包的合作策略，並獲得信任值得增加，所以在下一階段時此節點要傳送封包時也會優先被周圍節點所傳送。即使傳送封包需要耗費一定的成本且獲得的報酬不高，但是經由合作賽局的

長期報酬累計，終究會再某一階段得到累計的報酬，並以雙贏的互動關係於網路中生存。

5.5 第三方合作節點賽局

先前的分析皆假設傳送節點都會有第三方的合作節點做為備援，但是在實際情況下傳送節點不一定會有合作的備援節點存在，且倘若找到了備援節點，此備援節點也不一定會答應幫忙轉送封包，故需討論備援節點在之前存在與否對整個報酬產生影響的不同情況。

圖 55 是第三方合作節點示意圖，在 n_2 節點背離時如果傳送節點 n_1 能找到中繼節點 r_1 且能成功的轉送封包，故可得到報酬 S_1-C。若 r_1 也不轉送封包則繼續尋找 r_2 節點已請求轉送封包，直到備援節點尋找完為止。

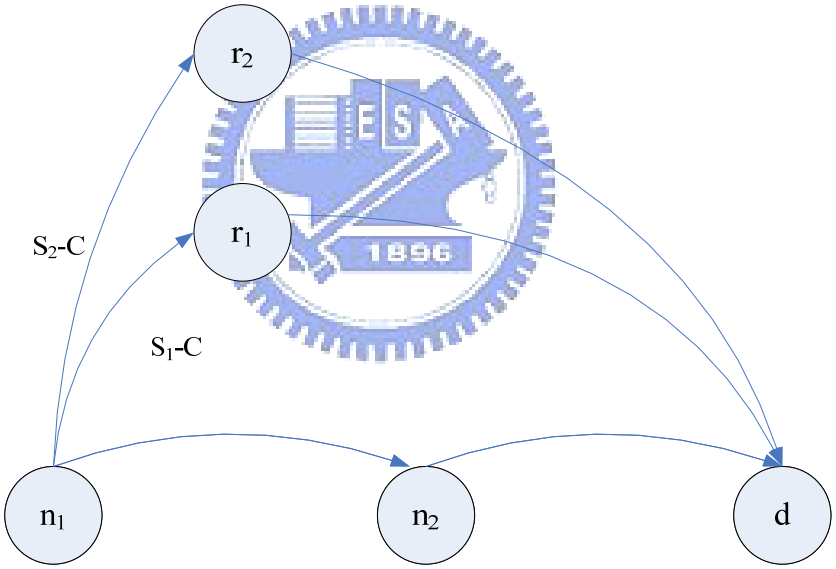


圖 55 第三方合作節點示意圖

5.5.1 存在合作備援節點

因為在信任證據的散佈中，傳送端已經有紀錄各別信任值和總信任值，所以在挑選中繼節點時可選擇比較值最大的節點傳輸。但是如果先前最受信任的節點決定不轉送的時候，傳送端必須尋求比較值第二大的節點轉送封包。故存在第三方節點時，當中繼節點背離時，傳送節點會尋求 r_1 傳送封包，r_1 會有 p_1 的機率傳送封包，有 $1\text{-}p_1$ 的機率不轉送封包。

推論 3:

$$LTP = Y(R-C) \geq STP = (X-1)(R-C)-C+ p_1(S_1-C)+(1-p_1)(-C)$$

$$= (X-1)(R-C)+ p_1S_1-2C$$

若存在 r_1 及 r_2 備援節點，則當中繼節點 n_2 背離時，傳送節點 n_1 可以選擇節點 r_1 要求轉送封包。如果 r_1 亦不轉送封包，n_1 只能進一步要求 r_2 轉送封包。最後倘若 r_2 也不轉送封包，則此賽局終止，傳送節點 n_1 也無法將封包傳往目的地。

推論 4:

$$LTP = Y(R-C) \geq STP = (X-1)(R-C)-C+ p_1(S_1-C)+(1-p_1)(-C)+p_2(S_2-C)+(1-p_2)(-C)$$

$$= (X-1)(R-C)+ p_1S_1+ p_2S_2-3C$$

根據推論 3 及推論 4，可以推導至 n 個節點，故可由比較值最大的備援節點開始傳輸，直到第 n 個節點願意轉送時此賽局停止，或者是到第 n 個節點皆不轉送，則傳送端浪費了轉送的成本，且沒有達成封包傳送。故可知當推論 5 成立時，永遠合作所得到的報酬會比暫時背離後所要找尋備援節點的報酬為大，所以節點為了避免此狀況，會傾向於合作。

推論 5:

$$LTP = Y(R-C) \geq STP = (X-1)(R-C)-C + p_1(S_1-C) + (1-p_1)(-C)+$$

$$p_2(S_2-C)+(1-p_2)(-C)+\ldots+p_n(S_n-C)+(1-p_n)(-C)$$

$$=(X-1)(R-C)\sum_{i=1}^{n} p_iS_i-(n+1)C$$

5.5.2 不存在合作備援節點

行動無基礎網路中因為節點的移動性，造成節點間的互動關係不一定存在，當節點移動至新的區域時，可能沒有和部分周圍節點有信任關係的互動，故需要找尋周圍可信任的節點作備援。這時可假設找到此新節點的機率為 q，找到備援節點後他願意轉送的機率為 p。當傳送端要找尋備援節點 r_1 時，有 q_1 的機率找到 r_1 節點，又此節點有 p_1 的機率可幫忙轉送封包，故可推導至以下的推論。

推論 6:

$$LTP = Y(R-C) \geq STP = (X-1)(R-C)-C+ q_1p_1(S_1-C)+(1- q_1p_1)(-C)$$

$$= (X-1)(R-C)+ q_1p_1S_1-2C$$

由推論 5 和推論 6 可知，傳送端可搜尋至 n 個備援節點，每個節點都有其答應轉送的機率。若第 n 個節點願意轉送，則此賽局終止且可達到目標。反之搜尋至第 n 個節點後亦無法將封包轉送，則會浪費要求轉送成本且無法將封包傳送至目的地。

推論 7:

$$LTP = Y(R-C) \geq STP = (X-1)(R-C)-C+q_1p_1(S_1-C)+(1- q_1p_1)(-C)+\ldots+$$

$$q_np_n(S_n-C)+ (1- q_np_n)(-C)$$

$$=(X-1)(R-C)\sum_{i=1}^{n} q_i p_i S_i - (n+1)C$$

經由推論 5 及推論 7 比較得知，當節點藉由總信任值的取得而獲得備援節點時，其報酬會比較大，故節點會傾向於存在合作節點多的行動無基礎網路中傳送封包，所以其行為會比較偏向合作以獲得長期的報酬。

5.6 信任賽局分析結論

經過賽局理論分析可知在連續封包傳輸以及互相封包傳輸的情況下，由推論 1 及 2 可知當一方背離時，雖然會得到短期報酬(X-1)(R-C)+ Θ，但是若節點的總信任值低於最小可信任值的話，則此節點會永遠被周圍節點所忽略。另一方雖然被背叛，但仍可得到 STP = (X-1)(R-C)+ pS-2C，且會傾向和別的節點合作。而由以下推論。

- $LTP = Y(R-C) \geq STP = (X-1)(R-C)+ pS-2C$
- $LTP = Y(R-C) \geq STP = (X-1)(R-C)+ \Theta$

可知節點長期合作後所得的總報酬會比背離後所得到的短期報酬為大，除此之外節點也會趨向於合作以獲得總信任值的提升，當它在將來想請求中繼節點幫忙轉送封包時，中繼節點會優先轉送封包。

第三方節點合作賽局可以推論本實驗的總信任值衡量可讓傳送節點得知備援節點的存在，故當傳送節點請求第一順位的中繼節點傳送封包但是被背叛時，可以及時的找尋總信任值次高的備援節點轉送封包。由推論 5 可知其

- $\mathrm{STP} = (X-1)(R-C)\sum_{i=1}^{n} p_i S_i - (n+1)C$

會大於推論 7 之沒有參考總信任值:

- $\mathrm{STP} = (X-1)(R-C)\sum_{i=1}^{n} q_i p_i S_i - (n+1)C$ ，

故節點若有備援節點存在於行動無基礎網路中，則此節點便不怕中繼節點的背叛，而可以選擇其他受信任的節點請求傳送封包服務。

結合以上的結論，可整理成以下的分析結果，可知:

(1) 行動網路節點會傾向於合作以增進其信任值，故節點會希望能藉由長期合作策略達到封包傳送，使得下一時間點時其節點若請求周圍節點傳送封包時，可以優先的被傳送。

(2) 於連續封包傳送賽局以及相互封包傳送賽局中，節點皆會以長期的合作作為優先考量，並期望能得到長期的合作報酬。

(3) 本研究之總信任值參考可讓節點在傳送封包之前就可以得到備援節點的資訊，故在封包傳送時如果信任值最大的節點背離時，節點可以及時的選擇第二順位的節點請求轉送封包，而不會有找不到備援節點的狀況發生。

第六章 結論與建議

6.1 憑證中心與信任證據比較

藉由以上的信任證據產生、散佈、衡量等方法可在行動無基礎網路中運行並解決自私節點與惡意節點問題。然而在既有的網際網路中，已經有類似的憑證中心在運作，但是實體的憑證中心在網路中已經建置好相關的階層結構，且工作站是長期存在於網路中，所以適合統一由中央實體憑證中心控管，並透過階層架構管理憑證資訊。

因為行動無基礎網路的架構為動態架構，節點的組成特性為隨機且臨時，故較適合研究所提之線上建構的信任證據。與實體憑證中心的不同點在於，行動無基礎網路的節點具有自我組成及管理的能力，故由節點做互相的管理及傳送封包衡量，更能反應網路中節點的行為。倘若將實體網路的憑證中心直接實行於行動無基礎網路中，會有眾多缺點存在，例如有些節點因為信號傳輸範圍的關係無法存取實體憑證中心的資料，且動態網路拓樸亦不適合單一管理。

表 21 為憑證中心與信任證據比較，由此可知信任證據適合在短暫式動態拓樸中施行。藉由節點各自產生憑證及互相驗證可以確保節點信任證據的真實性及傳送安全性，在加上個別信任值和總信任值的權重參照，能確實的反應網路節點的行為，使得節點須經由合作以讓周圍節點幫助轉送封包制目的節點，故可獲得雙贏的結果。

表 21 憑證中心與信任證據比較

	實體憑證中心	信任證據
架構	階層架構	平行架構
管理方式	中央統合管理	自我組成
適合網路環境	現有網際網路	行動無基礎網路
憑證建立	複雜	簡單
憑證管理	統一由憑證中心管理	由多個信任值高的節點管理
憑證存在時間	長期	短暫
單點脆弱的影響	高	低

6.2 研究結論

本研究提出了在行動無基礎網路中的信任證據方法，將身分認證、信任成員、信任節點、總信任值、和雜湊函數整合成信任證據，讓網路節點可以了解周圍節點的身分、被己方信任的程度、以及和其他節點互動後所賦予的總信任值。故在未來節點傳輸封包時，可以更可靠的信任節點的真實性和信任程度。其研究結論整理如下:

(1) 線上信任證據產生與散佈可以在行動無基礎網路中讓節點都有代表自己身份的證明，讓信任值高的周圍節點共同管理，且不用由中央實體方管理，故可以避免單點脆弱性的發生。

(2) 個別信任值與總信任值權重可使得節點透過己方對中繼節點的衡量以及參考周圍節點的衡量，所以可真實的反應中繼節點的行為，並及時的調整封包傳送策略。

(3) 透過其他節點評斷節點的信任程度，使得節點的參考性接近於他在行動無基礎網路中的社會化互動，讓自私節點和惡意節點藉由組信任值的降低自動被網路節點忽略。

(4) 賽局理論可分析雙方採取不同行動後所得到的報酬，縱使有一節點可以藉由一時的背離得到額外的報酬，但是在下一階段時別人不會跟他合作，故無法得到長期的報酬。此外研究可得知雖然合作所得到的短期報酬小於背離所獲得的報酬，但是經由不斷的合作累積小部分的報酬，在長期看來會超過背離所得到的報酬，故在此機制下節點會傾向於合作以獲取報酬並在網路中生存。

於實作模擬中，可以驗證信正證據運作可以解決自私節點與惡意節點問題，並得知當個別信任權重 $\alpha = 0.25$、總信任權重 $\beta = 0.75$ 為最佳的權重分配，故可將小部份的權重由己方節點衡量，且將大部份的權重交由具信任的節點衡量，如此一來可以順利運行於行動無基礎網路中，並解決自私節點以及惡意節點的問題。

6.3 未來研究方向

未來的研究方向可著重如下:

(1) 個別信任值的計算可利用評鑑推薦系統作衡量好壞的反應。

(2) 研究區塊驗證的範圍與包含的節點，以讓適當的節點個數做驗證，並使得尋找節點驗證所耗費的成本為最小。

(3) 賽局的節點封包傳送可考慮機會成本以及重要性的探討，讓忙碌節點傳送封包的價值增加。

經由機制的改良，期望將來能實地的運用到網路中，讓節點能夠透過合作達到效益的最大化，並排除不合作以及有惡意意圖的節點，使得這些節點雖然可存在於網路中，但是卻不會影響其他合作節點的運作。

參考文獻

[1] Eitan Altman and Tania Jimenez, “NS Simulator for beginners”, University de los Andes, Merida, Venezuela and ESSI, Sophia-Antipolis, France.

[2] John S Baras and Tao Jiang, “Cooperative Games, Phase Transitions on Graphs and Distributed Trust in MANET.”

[3] Vincent Buskens, “Social Networks and Trust”, Department of Sociology Utrecht University, Utrecht, The Netherlands.

[4] Srdjan Capkun, Levente Buttyan, and Jean-Pierre Hubaux, “Self-Organized Public-Key Management for Mobile Ad Hoc Networks”, IEEE Transactions On Mobile Computing, VOL. 2, No.1, January-March 2003.

[5] Hongmei Deng, Wei Li, Dharma P. Agrawal, “Routing Security in Wireless Ad Hoc Network”, IEEE Communications Magazine, 2002.

[6] Laurent Eschenauer, Virgil D,. Gligor, and John Baras, “On Trust Establishment in Mobile Ad Hoc Networks”, Electrical and Computer Engineering Department, University of Maryland College Park, MD20742, USA.

[7] Kevin Fall and Kannan Varadhan, “The ns Manual”, A Collaboration between researchers at UC Berkeley, LBL, USC/ISI, and Xerox PARC, December 7, 2005.

[8] Mark Felegyhazi and Jean-Pierre Hubaux, “Game Theory in Wireless Networks : A tutorial ”, EPFL-Switzerland.

[9] Robert Gibbons, “Game Theory for Applied Economists”, Princeton University Press, New Jersey.

[10] David Ingram, “An Evidence Based Architecture for Efficient, Attack-Resistant Computational Trust Dissemination in Peer-to-Peer Networks”, University of Cambridge Computer Laboratory, 15 JJ Thompson Avenue, Cambridge, CB3 0FD, United Kindom.

[11] Tao Jiang and John S. Baras, “Ant-based Adaptive Trust Evidence Distribution in MANET”, Institute for System Research , University of Maryland College Park, 20742.

[12] Allen B. MacKenzie and Stephen B. Wicker, Cornell, “Game Theory and the Design of Self-Configuring, Adaptive Wireless Networks”, Cornell University.

[13] C. Siva Ram Murthy, B.S. Manoj, “Ad Hoc Wireless Networks: Architectures and Protocols”, Prentice Hall PTR, 2004.

[14] Asad Amir Pirzada and Chris McDonald, “Establishing Trust in Pure Ad Hoc Networks”, School of Computer Science & Software Engineering, The University of Western Australia.

[15] Kui Ren, Tieyan Li, Zhiguo Wan, Fen Bao, Robert H. Deng, and Kwangjo Kim , “Highly Reliable Trust Establishment Scheme in Ad hoc Networks”, 1.International Center for Information Security, Information and Communication University, Daejeon, Korea 305732, 2.Institure for Infocomm Research, 21 Heng Mui Keng Terrace, Singapore 119613.

[16] Marcin Seredynski and Pascal Bouvry, “Evolution of Cooperation in Ad Hoc Networks under Game Theoretic Model”, University of Luxembourg 6, rue Coudenhove Kalergi L-1359, Luxembourg, Luxembourg.

[17] Oz Shy, “The Economics of Network Industries”.

[18] D. Subramanian, P. Druschel, J. Chen, “Ants and Reinforcement Learning: A case Study in Routing in Dynamic Networks”, In Proc. MILCOM, Atlantic City 1997.

[19] George Theodorakopoulos and John S. Baras, “Trust Evaluation in Ad-Hoc Networks”, Electronic and Computer Engineering Department and the Institute for Systems Research University of Maryland College Park, MD 20742.

[20] Daoxi Xiu and Zhaoyu Liu, “A Dynamic Trust Model for Pervasive Computing Environments”, Department of Software and Information Systems, University of

North Carolina at Charlotte.

[21] Dongmei Zhao, “Access Control in Ad Hoc Networks with Selfish Nodes”, Department of Electronic and Computing Engineering, McMaster University, Hamilton, Ontario, Canada L8S 4K1.

[22] C. Zouridaki, B. L. Mark, M. Hejmo and R. K. Thomas, “A Quantitative Trust Establishment Framework for Reliable Data Packet Delivery in MANETs”.

[23] http://www.gametheory.net