在隨意行動網路通訊架構下利用拜占庭協議演算法來防禦及偵測女巫攻擊

鄭勝鴻[1]、張世豪[2*]
[1, 2] 淡江大學資訊工程學系
[1] tommy81215@yahoo.com.tw、[2] shhchang@mail.tku.edu.tw

摘要

近年來網路科技快速蓬勃發展，現代人隨時隨地都能使用網路與其他使用者交流，不僅改變現代人生活的方式，也帶來更便利的生活。使用各種可攜式無線網路個人行動運算設備和使用有線網路相比，無線網路不僅能節省基礎設施的人力和花費，在架設的便利性及機動性也較有線網路來得更加優勢。

隨意行動網路 (Mobile Ad-Hoc Network, MANET) 是無線網路的其中一項分支。隨意行動網路具有能快速設置、動態拓樸的節點及缺少如轉接器、無線基地台(Access Point, AP)等基礎設施等特性，這些特性讓隨意行動網路能應用於特定的場景如軍事用途、搜救或緊急行動。基於路由協定，節點互相提供連結資訊並能共同建立完整傳輸路徑。但傳輸安全一直是隨意行動網路中的一項問題，起因於隨意行動網路的特性如連結公開的網路、因此缺少安全防線、去中心化的設置及路由協定中缺乏安全考慮的設計都讓 MANET 比有線網路更難於管理和抵禦利用這些弱點所形成的攻擊。

在本研究中針對隨意行動網路最常見的女巫攻擊(Sybil Attack)來做進一步的研究，女巫攻擊可能造成封包流量改向以及其他延伸影響。我們使用 NS3 模擬器來模擬一個基於共識機制的演算法拜占庭將軍問題協議(Byzantine Agreement Algorithm)來解決 Sybil attack 對於隨意行動網路的威脅。確保所有原來易遭受竄改的網路節點在傳輸過程中可以確保資料的完整性。我們在模擬的實驗中證明此了所提出的方法在網路及安全效能都能有較理想的表現。未來的目標在沒有網路基礎架構下，仍能保持通訊安全。

關鍵詞：資訊安全、隨意行動網路、拜占庭將軍問題協議、女巫攻擊、網路模擬

Defense and Detection of Sybil Attack Using Byzantine Agreement Algorithm in Mobile Ad Hoc Network

Sheng Hong Cheng[1], Shih-Hao Chang[2*]
[1, 2] Department of Computer Science and Information Engineering, Tamkang University, New Taipei City 25137, Taiwan (R.O.C.)
[1] tommy81215@yahoo.com.tw, [2] shhchang@mail.tku.edu.tw

[*] 通訊作者 (Corresponding author.)

Abstract

In recent years, modern rapid development of Internet technology has enabled people to use the Internet to communicate with each other anywhere, anytime and anytime. Not only changing the way people live in modern life, but also bringing about a more convenient life. The various portable wireless network personal mobile computing devices and the use of wired networks, compared to the wireless network can not only save the manpower and costs of the infrastructure, but also in the construction of the convenience and mobility are more advantages than the cable network.

In a mobile ad hoc network (MANET), MANET has nodes that can be quickly set up, dynamically topological, and lacks infrastructure such as adapters and wireless APs. These features allow MANETs to be used in specific scenarios such as Military use, search and rescue or emergency operations. Based on the routing protocol, nodes provide connection information to each other and can jointly establish a complete transmission path. But transmission security is a problem in MANET. MANET features such as open media, lack of security, non-centralized settings, and lack of security considerations in routing protocols make MANET more difficult to manage than wired networks. Resist attacks that exploit these weaknesses.

In this study, we conducted further research on the most common Sybil Attack of MANET. The witch attack may cause packet flow redirection and other extended effects. We utilize the simulation environment NS3 to simulate a consensus-based algorithm, the Byzantine Agreement Algorithm, to address the Sybil attack's threat to casual Internet networks. Ensure that all the original network nodes that are vulnerable to tampering can ensure the integrity of the data during transmission. We must demonstrate in the simulation experiment that this method can have ideal performance in both network and security performance. How to use a network form without an infrastructure to practice the security of a network in the form of an infrastructure network is the focus of this paper.

Keywords: Information Security, Mobile Ad Hoc Network, Byzantine Agreement Algorithm, Sybil Attack, Network Simulator

壹、前言

近年來，隨意無線網路 (Mobile Ad-Hoc Network, MANET) 技術的發展逐漸成為日常生活中不可或缺的網路連結架構。隨意無線網路與傳統的無線網路技術不同，主要區別是它不需要有固定的基礎設施，因此具有更好的靈活性。在 IEEE 802.11 定義兩種無

線網路架構[13]：基礎設施網路(Infrastructure network)和隨意無線網路，基礎設施網路也可以稱作主從式網路，它的特點就是有基地台的參與，基地台具備無線到有線的橋接功能，並且負責網路內所有的傳輸，包括同一個基本服務區域 (service area) 中所有行動節點之間的通訊，這表示所有的通訊都必須透過無線基地台 (Access Point, AP)，雖然這種作法比直接傳送耗費更多資源，但是它還是有兩個主要的優點：1. 基本服務區域被界定於基地台的傳輸範圍、2. 可協助行動節點節省電力。基本服務集 (Basic Service Set，簡稱 BSS) 是 802.11 網路的基本元件，它是由一組可彼此通訊的工作站所構成，只要位於基本服務區域內，工作站就可以跟同一個 BSS 中的其他成員通訊，但也因為通訊都必須透過無線基地台來完成，所以當無線基地台發生故障時將影響整體網路通訊。

隨意無線網路[8]是由一群希望相互通訊卻沒有固定基礎架構可用的通訊裝置所集合而成的網路，亦無事先已決定的可用路徑之組織。每一個行動節點動態 地找尋鄰近可以直接通信的其他行動節點，假定並非所有的行動節點都可以直接的與其他行動節點通訊時，則其它的行動節點必須扮演著中繼轉送(relay)的角色在網路之間傳遞資料封包。

而隨意無線網路屬於無線網路的一種[11]，在隨意無線網路之中的每個行動裝置都可以自由移動，隨時改變無線連結。每個行動裝置節點都必須協助轉發網路封包，即使這個封包是跟這個裝置無關的。因此，每個節點都扮演了路由器的角色。要建立一個隨意無線網路，最根本的挑戰在於讓每個行動裝置都能夠得到足夠的資訊，以協助保持網路資訊的暢通。在網路中重要的特徵是行動節點的快速移動造成網路拓撲的變化。網路中的節點是任意的，可以隨時加入或者是退出網路，亦或者是可以丟棄消息、偽造消息、停止工作等，還可能發生各種人為或非人為的故障。這種沒有明顯的防禦界線、沒有足夠物理保護、缺乏核心管理的特徵可能會使得節點容易遭受到有心人士的攻擊。

無線網路的蓬勃發展也引起惡意攻擊者的注意，其中女巫攻擊 (Sybil Attack) 透過建置大量虛假帳號以癱瘓系統是目前新興的網路攻擊行為之一[12]，女巫攻擊是一種對網路造成巨大危害的攻擊方式，會透過偽裝身分節點的方式，傳送虛假資料給其他節點。利用假扮多種身份的惡意節點大量傳播虛假訊息，以吸引更多的節點與它通信，造成路由訊息的混亂，再利用多重假身份改變所有傳輸路徑上的同一網路封包，使目標節點不能檢測出封包是否已受到干擾，達到攻擊的目的。

貳、文獻探討

2.1 隨意無線網路(Ad Hoc Network)

隨意無線網路擁有和有基礎架構的網際網路的安全性議題目標[10]，在大多數路由協議中，路由器交換關於網路拓撲的訊息以便建立節點之間的路由。這些訊息可能成為惡意攻擊者的目標，導致網路崩潰。路由協議有兩個威脅的來源，第一個來自外部攻擊

者。通過注入錯誤的路由訊息、重放舊的路由訊息或扭曲及竄改訊息的內容，攻擊者可以成功地對一個網路進行分區或者將過多的流量負載引入網路，導致重傳和低效路由。

第二種更嚴重的威脅是來自受損節點，這可能是向其他節點發布不正確的路由訊息。檢測這種不正確的訊息很困難，對於攻擊者來說，僅需要路由信息由每個節點簽名就會導致節點無法工作，因為節點已損壞能夠使用其私鑰生成有效的簽名。

為了防禦威脅，節點主要保護路由訊息在同樣的方法也保護了數據，例如：通過使用如數字簽名的密碼方案。但是，這個防禦對服務器受到攻擊的話無效。更糟糕的是，我們不能忽略了隨意無線網網路中節點受到攻擊的可能性。檢測受損節點通過路由訊息在自組織網路中也是困難的，因為它動態變化的拓撲結構：當一條路由訊息被發現無效時，訊息可以從一個受損的節點生成，或者由於拓撲結構的變化，它可能會變得無效。

對於隨意無線網路的安全我們考慮到以下幾點：有用性、機密性、完整性、認證性及不可否認性[14]。

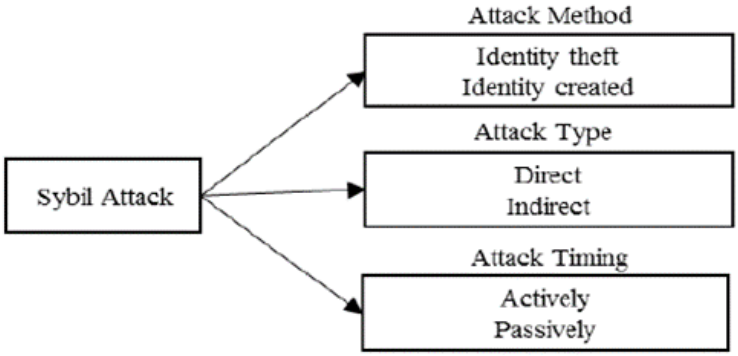
1. 有用性：確保在整個網路進行中的網路的存活率，像在實體層或媒體存取控制層可能干預或減小實體通道傳輸的效率，在網路層上可能搗亂了路徑的協定或導致網路的斷線，在應用層則會發生降低整個高水準的服務，像這個目標則建立一個任何層級都安全的網路架構。
2. 機密性：要確保在網路上正確的資訊不會暴露在沒有經過認證的實體使用者上，網路上傳輸的資訊像是軍事上的或戰略上這類極 機密的資訊，會特別在機密上有所要求，尤其在傳送的路徑上也需極機密的保護，要保障傳送路徑的安全不會被竊聽、攔截或破壞。
3. 完整性：要確保傳送者傳到接受者的資訊要是一樣的，一個資訊有可能在傳送過程遭受惡意攻擊或傳送的環境被擾亂而導致資訊的失敗或遺失。
4. 認證性：要確保每一個終端節點在整個網路通訊都是經過認證的，如果沒有經過認證的話，攻擊者可能會偽裝某一節點對於整個網路資源作非法的存取，甚至干預了整個網路的運作。
5. 不可否認性：要確保在傳送者傳送了原始訊息不能否認曾經傳過這樣的訊息時，假如甲收到了由乙傳送過來的錯誤訊息，乙不可以否認沒有傳過這個錯誤的訊息，以證明責任的歸屬。

2.2 女巫攻擊(Sybil Attack)

女巫攻擊(Sybil Attack)是 2002 年由 John R. Douceur 在《the Sybil Attack》[4]文中提出的，它是作用於對等（Peer-to-Peer,簡稱 P2P）網路中的一種攻擊形式，攻擊者利用單個節點來偽造多個身份存在於 P2P 網路中，從而達到削弱網路的冗餘性，降低網路安全性，監視或干擾網路正常活動等目的。

在 P2P 網路中，為了解決來自惡意節點或者節點失效帶來的安全威脅，通常會引入

冗餘備份機制，將運算或存儲任務備份到多個節點上，或者將一個完整的任務分割存儲在多個節點上。正常情況下，一個設備實體代表一個節點，一個節點由一個身份識別(Identification, ID) 來標識身份。然而，在缺少可信賴的節點身份認證機構的 P2P 網路中，難以保證所備份的多個節點是不同的實體。攻擊者可以通過只部署一個實體，向網路中廣播多個身份 ID，來充當多個不同的節點，這些偽造的身份一般被稱為 Sybil 節點[3][7]。 Sybil 節點為攻擊者爭取了更多的網路控制權，一旦用戶查詢資源的路徑經過這些 Sybil 節點，攻擊者可以干擾查詢、返回錯誤結果，甚至拒絕回復。下面將介紹 Sybil Attack 的攻擊方法、類型及時間(如圖一)



圖一：Sybil Attack 的攻擊方法、類型、時間

2.2.1 女巫攻擊的攻擊方法、類型及時間[5]

偽造身份：

一個女巫攻擊者可以生成任意的身份，然後再對附近的節點攻擊。

盜用身份：

盜用原本持有此身份的網路實體。

直接通信：

女巫(Sybil)節點直接與合法節點進行通信。當運作與正常的節點發送一個訊息通過女巫攻擊的節點時，此具女巫攻擊的節點中的會監聽這個消息。反觀，從所有女巫節點發送出的消息事實上是由同一個女巫攻擊的惡意節點發出的。

間接通信：

發送出女巫攻擊節點的消息都是由已經被女巫惡意節點妥協的網路節點進行路由轉發的，這個惡意節點假裝把這個消息發送給女巫節點，而事實上就是這個惡意節點自

己接收或者攔截了這個消息。

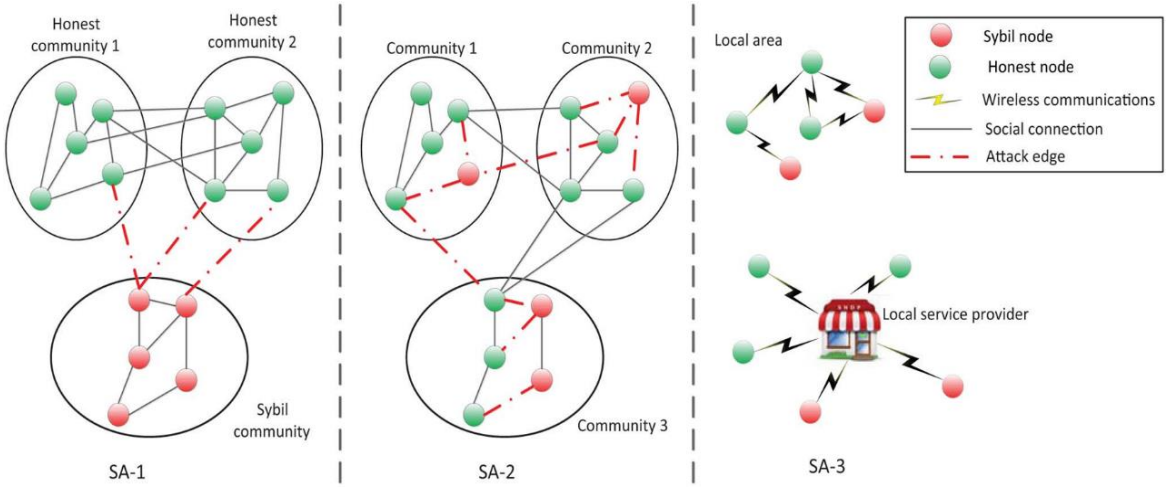
同時攻擊：

女巫攻擊者將其所有的女巫身份一次性的同時攻擊同一網路架構通信中的節點。

非同時攻擊：

女巫攻擊者在一個特定的時間裡使用不同的身份，而在另外一個時間裡讓這些身份另外的女巫身份出現，看起來就像網路正常的節點離開與加入。

2.2.2 女巫攻擊的網路型態



圖二：女巫攻擊的網路型態

女巫攻擊 (Sybil Attack) 在網路中被定義為三種型態 SA-1 、SA-2 及 SA-3，圖二為三種網路類型的示意圖，來更清楚理解三種不同類型的差別[9]。

(1) SA-1

Sybil 節點彼此連結形成一個網路，透過 attack edge 去跟運作正常的節點去做連結，但是 SA-1 的連接能力不強，因為 Sybil 節點只能跟附近的節點連接，所以它的 attack edges 的數量相對比較少，是受到距離限制的，SA-1 的攻擊者通常存在於感知網域和社交網域，在很多情況下，從用戶的行為是難區分是否為 Sybil 攻擊。

(2) SA-2

與 SA-1 不同，SA-2 能建立社交連結，此連結中的節點不僅可以包括女巫 Sybil 節點也可以是一般正常的節點，因為 SA-2 的特點就是強於一般一對一的社交結構，因此 attack edges 的數量相對較多，攻擊能力也比較強 SA-2 的攻擊目標是傳播垃圾郵件，廣告，和惡意軟體;竊取和侵犯用戶的隱私;和惡意操縱系統的信譽。

(3) SA-3

SA-3 女巫攻擊者大多存在於行動網域中，主要攻擊目標類似於 SA-2。SA-3 的攻擊都是在短期或是固定時間，由於行動網域屬於動態移動因此用戶間沒辦法持續連結或是它是屬於間歇性的連結，所以對於節點結構或是拓樸來說都會隨時變動所以不容易防禦。此外，行動網路較無法用由中央發給認證 centralized authority。 因此，行動網路中的行為模式並不容易獲得防禦導致 SA-3 的防禦難度比較大。

2.3 拜占庭將軍問題(Byzantine Generals Problem)

「拜占庭將軍問題」（Byzantine Generals Problem）是一個建立於共識機制解決的實例[6]，由萊斯利·蘭波特在其同名論文中提出的分散式對等網路通訊容錯問題。拜占庭為過去東羅馬帝國的首都，現在位於土耳其的伊斯坦堡。由於當時拜占庭羅馬帝國的國土遼闊，基於防禦目的，每個軍隊都分隔遙遠，因此將軍間只能靠信差傳遞消息。於戰爭時，拜占庭帝國軍隊的將軍們必須全體一致的決定是否攻擊某一支敵軍，因為唯有達成一致的行動才能獲致勝利。將軍中若存在叛徒，叛徒可以採取行動以欺騙某些將軍進行進攻行動，或致使他們無法做出決定，缺乏一致行動的結果則將註定戰事的失利。

拜占庭將軍問題的兩種解決演算法，口頭消息(Oral Messages)和簽名消息(Signed Messages)，口頭消息的算法在共識運作為訊息在網路中節點間互相交換後，由各節點列出所有得到的訊息，以大多數的結果作為解決辦法。主要依據法定多數（quorum）的決定，一個節點代表一票，以少數服從多數的方式實現至多容錯量以不超過全部節點數的 1/3，意即如果有超過 2/3 的正常節點，整個網路就便可正常運作，必須滿足 $R \geq 3F + 1$ 的規則，R：節點總數，F：有問題節點總數。

簽名消息的算法在除了滿足口頭消息要求外還需滿足另外的兩個條件 1.簽名不可被偽造，一旦被篡改即可發現 2.任何人都可以驗證將軍簽名的可靠性。在算法中將軍將簽了自己姓名的消息廣播發給所有副官(V:0;V 是命令，0 代表自己的身份)，副官在進而發送給其他的副官(簽名消息的算法中，讓副官簽名是確認其收到了該消息)。假如 A 是叛徒。A 給 B 發進攻，給 C 發撤退（都被 A 簽名），B 比較從 C 發來的命令（撤退，該命令被 C 簽名了）知 A 是叛徒。C 比較從 B 發來的命令（進攻，該命令由 B 簽名），知 A 是叛徒。

參、方法

3.1 實用拜占庭容錯(Practical Byzantine Fault Tolerance)

為了解決節點可能被惡意攻擊者造成的危害，在此研究中利用一種共識機制以及入

侵容忍體系的一種演算法，在隨意行動網路中加入拜占庭容錯算法(Practical Byzantine Fault Tolerance)來解決惡意節點可能對網路架構的危害。

PBFT[1][2]是 Practical Byzantine Fault Tolerance 的縮寫，意為實用拜占庭容錯算法。該算法是 Miguel Castro (卡斯特羅)和 Barbara Liskov（利斯科夫）在 1999 年提出來的，該論文發表在 1999 年的 Operating Systems Design and Implementation 上（OSDI99）解決了原始拜占庭容錯算法效率不高的問題，將算法複雜度由指數級降低到多項式級，使得拜占庭容錯算法在實際系統應用中變得可行。

其思想淵源來自拜占庭將軍問題，是一種解決分布式系統容錯問題的通用方案。PBFT 是一種狀態機複製算法（state machine replication），即服務作為狀態機建立模型，並且在網路系統的不同節點進行副本複制，每一個狀態機的副本都保存了服務的狀態，同時也實現了服務的操作。副本的集合用 R 表示，{0, …, |R| − 1} 的一個整數表示副本。我們假設|R| = 3f + 1，R 是系統中的總副本數，f 是允許出現故障及錯誤的副本數。換句話說，當存在 f 個故障及錯誤的副本時必須保證存在至少 3f+1 個副本數量，這樣才能保證在網路系統中提供安全性。這麼多數量的副本是必需的，因為在 R-f 個副本通訊後系統必須做出正確判斷，由於 f 個副本有可能失效而不發回回應。儘管如此，網路系統仍舊需要足夠數量的非失效副本回應，並且這些非失效副本的回應數量必須超過失效副本的回應數量，即 R-2f>f，因此得到 R>3f。

所有的副本在一個被稱為視圖（View）的輪替轉換過程中運作。在某個視圖中，一個副本作為主節點（primary），其他的副本作為備份（backups）。視圖是連續編號的整數。副本 0 到副本 R-1 依次當主節點，當每一次 view change 發生時主節點由公式 p = v mod |R|計算得到，這裡 v 是視圖編號，p 是副本編號，|R|是副本集合的個數。當主節點失效的時候就需要啟動視圖更換（view change）過程。

客户端 c 向主節點發送<REQUEST,o,t,c>請求執行狀態機操作 o，這裏時間戳 t 用來保證客户端請求只會執行一次。客户端 c 發出請求的時間戳是全序關係排列的，後續發出的請求比早先發出的請求擁有更高的時間戳。例如，請求發起時的本地時間值可以作為時間戳。

每個由副本節點發給客户端的消息都包含了當前的視圖編號，使得客户端能夠跟蹤視圖編號，從而進一步推算出當前主節點的編號。客户端通過點對點消息向它自己認為的主節點發送請求，然後主節點自動將該請求向所有備份節點進行廣播。

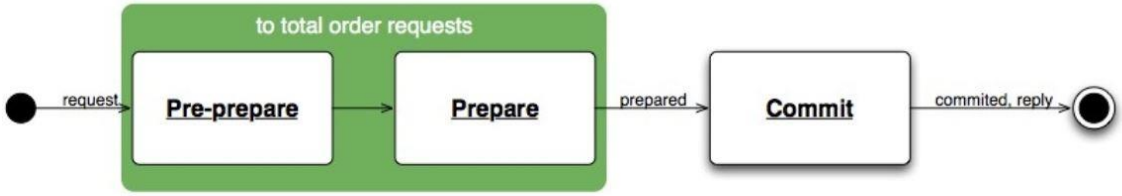
副本發給客户端的回應為<REPLY,v,t,c,i,r>，v 是視圖編號，t 是時間戳，i 是副本的編號，r 是請求執行的結果。

客户端等待 f+1 個從不同副本得到的同樣回應，同樣回應需要保證簽名正確，並且具有同樣的時間戳 t 和執行結果 r。這樣客户端才能把 r 作為正確的執行結果，因為失效的副本節點不超過 f 個，所以 f+1 個副本的一致回應必定能夠保證結果是正確有效的。

如果客户端沒有在有限時間內收到回覆，請求將向所有副本節點進行廣播。如果請求已經在副本節點處理過了，副本就向客户端重發一遍執行結果。如果請求沒有在副本

節點處理過，該副本節點將把請求轉發給主節點。如果主節點沒有將該請求進行廣播，那麼就有認為主節點失效，如果有足夠多的副本節點認為主節點失效，則會觸發一次視圖變更。

3.2 PFT 算法流程



圖三：PBFT 流程圖

其步驟流程如下(如圖三)：

(1) 取一個副本作為主節點，其他的副本作為備份
(2) 用戶端向主節點發送使用服務操作的請求
(3) 主節點通過廣播將請求發送給其他副本
(4) 所有副本執行請求並將結果發回用戶端
(5) 用戶端需要等待 F+1 個不同副本節點發回相同的結果，作為整個操作的最終結果

算法對每個副本節點提出了兩個限定條件：

(1) 所有節點必須是確定性的，也就是說，在給定狀態和參數相同的情況下，操作執行的結果必須相同。
(2) 所有節點必須從相同的狀態開始執行。在這兩個限定條件下，即使失效的副本節點存在，算法對所有非失效副本節點的請求執行總順序達成一致，從而保證安全性。

當主節點 p 收到客戶端的請求 m，主節點將該請求向所有副本節點進行廣播，進行三階段協議(three-phase protocol)。預準備(pre-prepare)、準備(prepare)和確認(commit) 。預準備和準備兩個階段用來確保同一個視圖中請求發送的時序性(即使對請求進行排序的主節點失效了)，準備和確認兩個階段用來確保在不同的視圖之間的確認請求是嚴格排序的。

所有的副本在一個被稱為視圖（View）的輪替轉換過程中運作。在某個視圖中，一個副本作為主節點(primary)，其他的副本作為備份(backups)。視圖是連續編號的整數。副本 0 到副本 R-1 依次當主節點，當每一次 view change 發生時主節點由公式 $p = v \bmod |R|$ 計算得到，這裡 v 是視圖編號，p 是副本編號，|R|是副本集合的個數。當主節點失效

的時候就需要啟動視圖更換（view change）程序，即重新尋找主節點的程序。

客户端 c 向主節點發送<REQUEST,o,t,c>請求，執行狀態機操作 o，這裡時間戳 t 用來保證客户端請求只會執行一次。

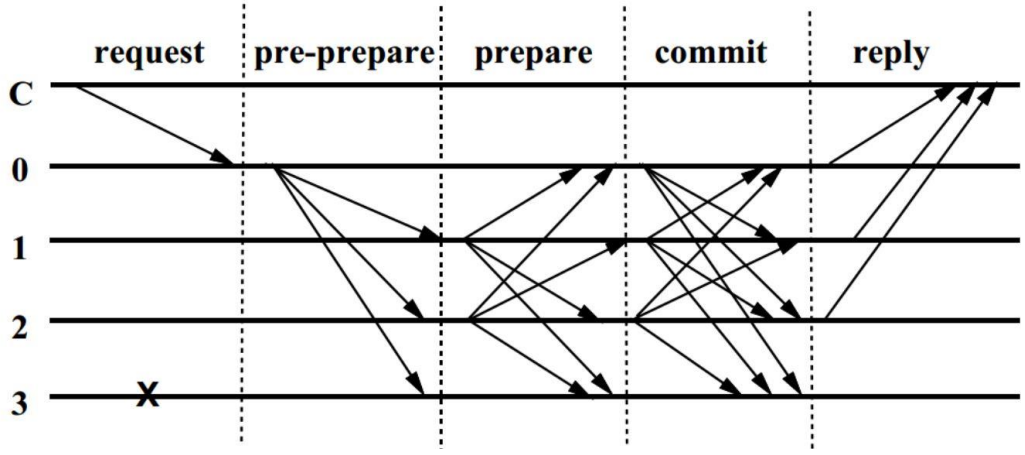
每個由副本節點發給客户端的消息都包含了當前的視圖編號，使得客户端能夠跟蹤視圖編號，從而進一步推算出當前主節點的編號。客户端通過點對點消息向它自己認為的主節點發送請求，然後主節點自動將該請求向所有備份節點進行廣播。

副本發給客户端的回應為<REPLY,v,t,c,i,r>，v 是視圖編號，t 是時間戳，i 是副本的編號，r 是請求執行的結果。

客户端等待 f+1 個從不同副本得到的同樣回應，同樣回應需要保證簽名正確，並且具有同樣的時間戳 t 和執行結果 r。這樣客户端才能把 r 作為正確的執行結果，因為失效的副本節點不超過 f 個，所以 f+1 個副本的一致回應必定能夠保證結果是正確有效的。

如果客户端沒有在有限時間內收到回覆，請求將向所有副本節點進行廣播。如果請求已經在副本節點處理過了，副本就向客户端重發一遍執行結果。如果請求沒有在副本節點處理過，該副本節點將把請求轉發給主節點。如果主節點沒有將該請求進行廣播，那麼就有認為主節點失效，如果有足夠多的副本節點認為主節點失效，則會觸發一次視圖變更。

圖四展示了在沒有發生主節點失效的情況下算法的執行流程，其中副本 0 是主節點，副本 3 是失效節點，而 C 是客户端。



圖四：算法節點的執行流程圖

3.2.1 預準備(pre-prepare)

在預準備階段，主節點分配一個串行號 n 給收到的請求，然後向所有備份節點羣發預準備消息，預準備消息的格式為 <PRE-PREPARE,v,n,d,m>，這裏 v 是視圖編號，m 是客户端發送的請求消息，d 是請求消息 m 的摘要。

只有滿足以下條件，各個備份節點才會接受一個預準備消息：

1. 請求和預準備消息的簽名正確，並且 d 與 m 的摘要一致。
2. 當前視圖編號是 v。
3. 該備份節點從未在視圖 v 中接受過序號為 n 但是摘要 d 不同的消息 m。
4. 預準備消息的序號 n 必須在水線（watermark）上下限 h 和 H 之間。

水線存在的意義在於防止一個失效節點使用一個很大的序號消耗序號空間。

3.2.2 準備(prepare)

如果備份節點 i 接受了預準備消息<PRE-PREPARE,v,n,d,m>，則進入準備階段。在準備階段的同時，該節點向所有副本節點發送準備消息<PREPARE,v,n,d,i>，並且將預準備消息和準備消息寫入自己的消息日誌。包括主節點在內的所有副本節點在收到準備消息之後，對消息的簽名是否正確，視圖編號是否一致，以及消息序號是否滿足水線限制這三個條件進行驗證，如果驗證通過則把這個準備消息寫入消息日誌中。

我們定義準備階段完成的標誌為副本節點 i 將(m,v,n,i)記入其消息日誌，其中 m 是請求內容，預準備消息 m 在視圖 v 中的編號 n，以及 2f 個從不同副本節點收到的與預準備消息一致的準備消息。每個副本節點驗證預準備和準備消息的一致性主要檢查：視圖編號 v、消息序號 n 和摘要 d。

預準備階段和準備階段確保所有正常節點對同一個視圖中的請求序號達成一致。接下去是對這個結論的形式化證明：如果 prepared(m,v,n,i)為真，則 prepared(m',v,n,j)必不成立，這就意味着至少 f+1 個正常節點在視圖 v 的預準備或者準備階段發送了序號為 n 的消息 m。

3.2.3 確認(commit)

當(m,v,n,i)條件為真的時候，副本 i 將 <COMMIT,v,n,D(m),i> 向其他副本節點廣播，於是就進入了確認階段。每個副本接受確認消息的條件是：

(1) 簽名正確；
(2) 消息的視圖編號與節點的當前視圖編號一致；
(3) 消息的序號 n 滿足水線條件，在 h 和 H 之間。
(4) 一旦確認消息的接受條件滿足了，則該副本節點將確認消息寫入消息日誌中。

我們定義確認完成 committed(m,v,n)為真的條件為：任意 f+1 個正常副本節點集合中的所有副本 i 其 prepared(m,v,n,i)為真；本地確認完成 committed-local(m,v,n,i)為真的條件為：prepared(m,v,n,i)為真，並且 i 已經接受了 2f+1 個確認(包括自身在內)與預準備消息一致。確認與預準備消息一致的條件是具有相同的視圖編號、消息序號和消息摘要。

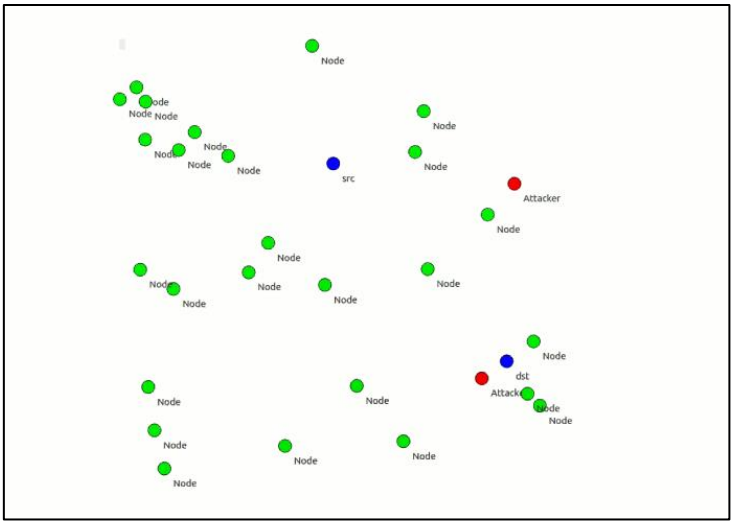
每個副本節點 i 在 committed-local(m,v,n,i)為真之後執行 m 的請求，並且 i 的狀態反

映了所有編號小於 n 的請求依次順序執行。這就確保了所有正常節點以同樣的順序執行所有請求，這樣就保證了算法的正確性(safety)。在完成請求的操作之後，每個副本節點都向客户端發送回覆。副本節點會把時間戳比已回覆時間戳更小的請求丟棄，以保證請求只會被執行一次。

肆、實驗及結果

4.1 NS3 模擬

本實驗使用 NS3 網路模擬器來實驗，實驗環境設置一個基於 AODV 協議的 Manet 網路系統，在網路中設置三十個一般合法節點以及兩個 Sybil Attack 的惡意節點，所有節點的移動，以五公尺每秒採隨機移動的方式傳送訊息使用廣播的形式去給附近節點，然後設置源節點傳送訊息給目標節點。圖五為此研究中節點的模擬設置。

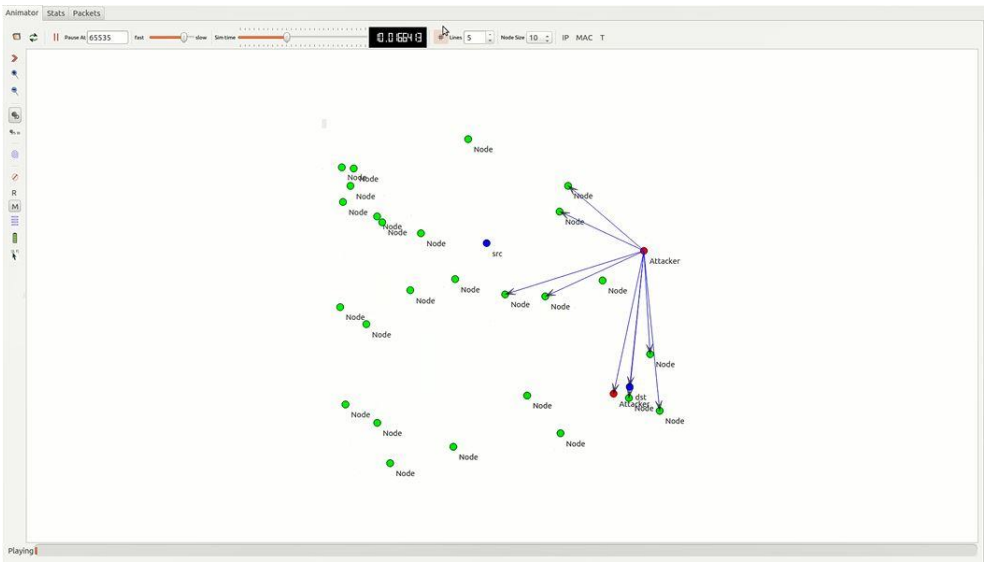


圖五：節點模擬設置

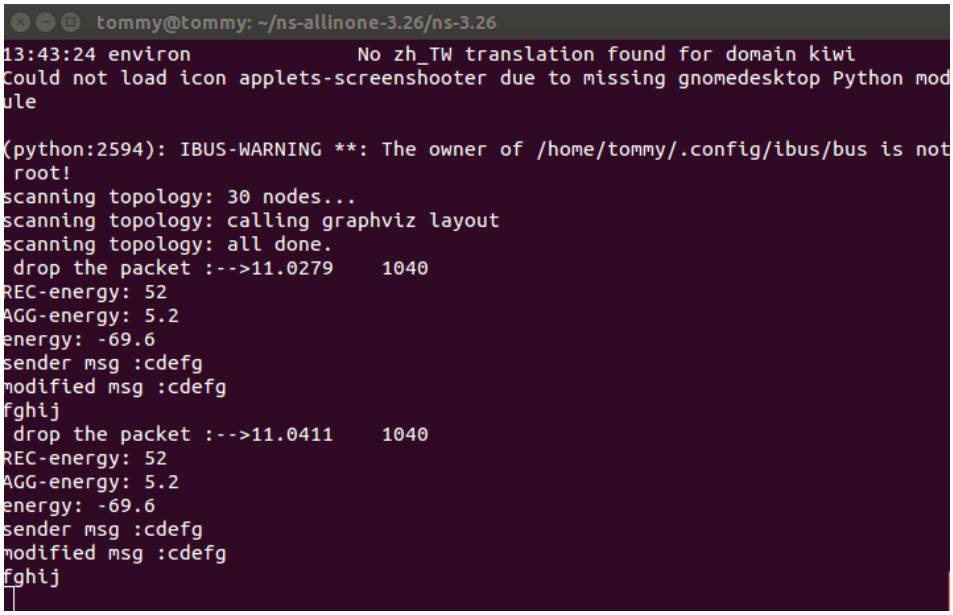
4.2 Sybil 節點的攻擊方式

Sybil 節點大量傳播虛假訊息，以吸引附近更多的節點與它通信，造成路由訊息的混亂，達到攻擊的目的攻擊者利用多重身份改變所有傳輸路徑上的同一數據包，使目標節點不能檢測出封包是否已受到乾擾。假設設置源節點傳遞的訊息為“abc”，則 Sybil 節點改變訊息+3 為 cde ，例如：a+3=c，b+3=d ，c+3=e，所以得出 cde。圖六是在模擬過過程中 Sybil 的惡意節點會發出假消息來欺騙附近的節點，讓附近節點幫忙轉發假消息。

圖七為經 Sybil 攻擊後，成功欺騙網路中的節點，最後目的地節點收到假消息。



圖六：模擬 Sybil 攻擊

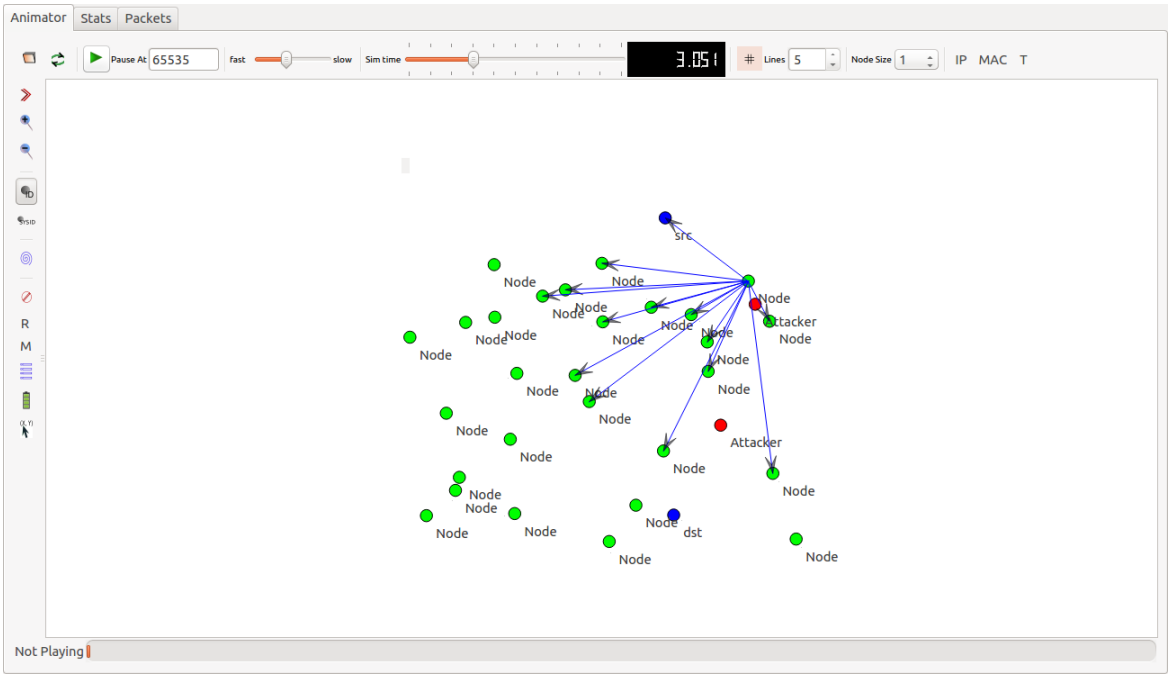


圖七：Sybil 節點成功竄改消息

4.3 PBFT 防禦機制

在本研究中使用，實用拜占庭容錯算法(Practical Byzantine Fault Tolerance)後，節點互相傳遞消息後，可以偵測出 SYBIL 惡意節點，然後加以判斷。假設該節點經節點彼此

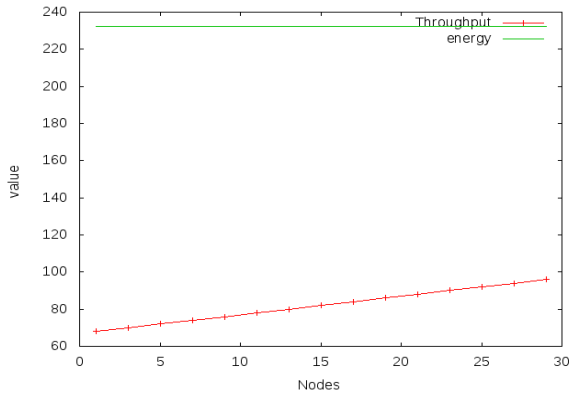
轉發以及驗證為惡意節點，那系統就會判斷此節點為失效節點，將不再與該節點在做通信或是幫它轉發消息的動作。圖八為判斷紅色節點為惡意攻擊的節點，將不再與其通信及轉發消息。



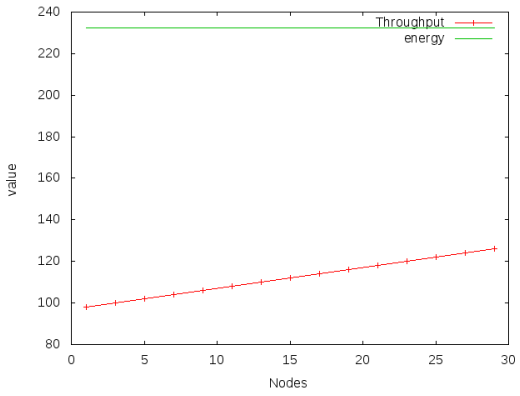
圖八：防禦及偵測惡意攻擊

4.4 節點吞吐量比較

在本研究中分析使用 PBFT 機制和未使用 PBFT 機制的吞吐量比較，在模擬過程中能量一樣的情況下，女巫攻擊網路後每個節點的吞吐量的數值為 60 到 100 之間，而使用 PBFT 機制後防禦網路的節點吞吐量則是 90-130 之間。圖九中是在 30 個節點中女巫攻擊吞吐量的數值。圖十是在 30 個節點中女巫攻擊的惡意節點工及網路使用 PBFT 機制防禦的吞吐量。



圖九：女巫攻擊的吞吐量



圖十：使用 PBFT 機制的吞吐量

伍、結論

在本研究中針對 MANET 最常見的女巫攻擊(Sybil attack)來做進一步的研究，他可能造成封包流量改向以及其他延伸影響。在隨意行動網路中一但路徑建立，要傳送的訊息在源節點和目的地節點之間傳輸。在這種情況下，可能發生攻擊或者是傳送的訊息內容被修改、注入及竊聽等。

我們使用模擬環境來模擬一個基於共識機制以及入侵容忍體系的演算法實用拜占庭容錯算法(Practical Byzantine Fault Tolerance)來解決 Sybil attack 對於隨意行動網路的威脅。確保所有原來易遭受竄改的網路節點在傳輸過程中可以確保資料的完整性。我們在模擬的實驗中須證明此方法在網路及安全效能都能有理想的表現。

惡意使用者(Malicious User) 會利用大量多重虛擬身分企圖控制信譽系統的評比結果，這類型攻擊會影響正常使用者的信譽評比，並藉此獲得不當利益，操控使用者於網路上信譽評比的攻擊行為，已儼然成為一個不可輕忽的重大議題。

在本研究使用的演算法，在隨意行動網路中正常節點透過互相投票的方式可以偵測出女巫攻擊的節點，進而防禦可將正常使用者與惡意使用者成功辨別，並對於隨意行動網路的使用者提供更加安全可靠的使用環境。

參考文獻

[1] M. Castro and B. Liskov, "Practical Byzantine Fault Tolerance," *Proceedings of the Third Symposium on Operating Systems Design and Implementation*, pp.1-14, Feb. 1999.

[2] M. Castor and B. Liskov, "Practical Byzantine Fault Tolerance and Proactive Recovery," *ACM Transactions on Computer Systems (TOCS)*, vol. 20, pp. 398–461, Nov. 2002.

[3] C. R. Davis, J. M. Fernandez, S. Neville and J. McHung, "Sybil attacks as a mitigation

strategy against the storm botnet," *2008 3rd International Conference on Malicious and Unwanted Software (MALWARE)*, pp. 32-40, Oct. 2008.

[4] J. R. Douceur, "The sybil attack," *Proceedings of the International Workshop on Peer-to-Peer Systems*, Springer, Berlin, Heidelberg, pp.251-260, 2002.

[5] A. Gupta, D. Sukheja and A. Tiwari, "Impact of Sybil Attack and Security Threat in Mobile Adhoc Network," *Proceedings of the International Journal of Computer Applications*, vol. 124, pp.5-12, Aug. 2015.

[6] L. Lamport, R. Shostak and M. Pease, "The Byzantine Generals Problem," *ACM Transactions on Programming Languages and Systems (TOPLAS)*, vol. 4, pp. 382-401, July. 1982.

[7] J. Newsome, E. Shi, D. Song and A. Perrig, "The Sybil attack in sensor networks: analysis & defenses," *Proceedings of the 3rd international symposium on Information processing in sensor networks*, pp.259-268, Apr. 2004.

[8] R. Ramanathan and J. Redi, "A Brief Overview of AD Hoc Networks:Challenges And Directions," *IEEE communication Magazine 50th Anniversary Commemorative Issue*, pp. 20-22, May, 2002.

[9] K. Zhang, X. Liang, R. Lu and X. Shen, "Sybil Attacks and Their Defenses in the Internet of Things," *Proceedings of the IEEE Internet of Things Journal*, vol. 1, pp.372-383, Oct. 2014.

[10] L. Zhou and Z. J. Haas, "Securing ad hoc networks," *IEEE Network*, vol.13, no.6, pp.24-30, 1999.

[11] https://zh.wikipedia.org/wiki/%E9%9A%A8%E5%BB%BA%E5%8D%B3%E9%80%A3%E7%B6%B2%E8%B7%AF

[12] 吳恭漢，"無線感測網路中女巫攻擊偵測之研究"，*碩士論文*，國立臺北教育大學，2016.

[13] 郭澄宇，"基於 NS2 網路模擬器之隨意任意網路資料傳輸模組之開發"，*碩士論文*，中華大學， 2010。

[14] 黃秀園、李正吉、黃國祐，"隨意型無線網路之安全技術"，*會議論文*，亞洲大學電腦與通訊學系， 2006。