健全且普及之行動隨意無線網路安全環境

隨意無線網路(Ad Hoc networks)是由一群無固定基礎建設的行動通訊裝置集合而成，在這樣的網路環境中面臨許多挑戰，如遭受到主動及被動的攻擊、須提供即時與隨地之服務。因此本研究提出以門檻值憑證中心之架構為基礎，應用橢圓曲線密碼系統，建立適合隨意無線網路之公開金鑰基礎建設，使網路中被授命之節點(稱之MAPC)能聯合簽署憑證，達到隨意無線網路之安全目標。本研究以橢圓曲線進行加解密，並以ECDSA 進行數位簽署，如此與RSA 比較大幅度降低運算時間及金鑰長度；同時亦採用秘密分享更新及定期對MAPC 進行稽核之方式，來抵抗各種攻擊；另外針對隨意無線網路節點之移動特性，設計一MAPC 個數、門檻值為可變動的網路環境，使隨意無線網路之公開金鑰基礎建設更具可行性。隨意無線網路的無線、移動性等特性，導致安全控管成為隨意無線網路中較弱的一環，公開金鑰基礎建設即提供了金匙分配及身分認證的安全機制，使得網路內之訊息傳遞能達成機密性、認證性、完整性及不可否認性之安全目標。