台灣網路智能學會

110 學年度博碩士論文得獎名單

碩士論文獎 5 名

論文題目：植基於圖異常偵測並以情資為特徵之 APT 攻擊偵測系統

學校：國立中山大學 資訊工程學系 資訊安全碩士班

研究生：張郢展

指導教授：范俊逸

摘要：

現今進階持續性威脅攻擊中，駭客結合多種防禦迴避技術來躲避傳統防毒軟體偵測，例如無檔案式惡意程式（Fileless Malware）結合離地攻擊（Living Off the Land，LOL）以及合法雲服務濫用，使得企業紛紛轉而採用端點偵測及回應（Endpoint Detection and Response，EDR），EDR 工具將事件記錄與已知的攻擊技術相匹配，藉此偵測出潛在的威脅。然而，EDR 工具卻存在產生大量警告誤報的缺點，使得資安維護人員與分析人員被迫增加額外大量的分析成本。

在本文中，我們提出植基於圖的異常偵測系統，藉由輸入正常行為所建構具有威脅情資的出處圖至本系統，學習該圖中的潛在結構化資訊，達到偵測主機上的異常行為。結果顯示所提出的系統能有效偵測出異常的事件記錄，此外將警告誤報數量減少了高達 97.67%，除了大幅降低資安維護人員因分析記錄而造成的龐大負擔，並且說明基於圖神經網路的異常偵測能力優於傳統神經網路。

關鍵字：進階持續性威脅、離地攻擊、端點偵測及回應、威脅情資、出處圖、異常偵測、圖神經網路

論文題目：基於低軌衛星之認證協定與金鑰協議

學校：國立中山大學 資訊工程學系 資訊安全碩士班

研究生：王楓鈞

指導教授：范俊逸

摘要：

在 5G 標準發展時，各項研究著重於保護使用者身分隱私，最終制定出使用公鑰系統加密使用者身分，加密後稱作 SUPI，搭配 GUTI，解決了長久以來因 IMSI 的竊取導致使用者身分洩露問題。然而在~6G~時，隨著量子電腦的發展，現行的公鑰系統將可能存在安全性上的疑慮，故以其加密之 SUPI 可能已不安全。除此之外，利用公鑰加密時耗費較多資源來運算。

在 6G 時，網路架構將會拓展至空中，在使用第三方衛星基地台時，既需透過衛星與使用者連線認證，分辨不同電信業者之流量，又必須保護使用者隱私。本研究提出了基於雜湊函數之認證協定，使用者連上第三方所提供之低軌道衛星基地台，並透過衛星基地台與地面之核心網路認證。在使用第三方所提供之低軌道衛星基地台時，低軌道衛星基地台無法透過認證過程中各項資訊連結到使用者，進而追蹤使用者動態。在確保使用者隱私的前提下，低軌道衛星基地台能辨別使用者所屬之電信業者，將連線請求導向相應之核心網路（CN）完成認證。相較於公開金鑰加密系統，基於雜湊之認證協定能降低計算成本，亦能抵禦未來可能之量子電腦攻擊。

關鍵字：基於雜湊函數之認證、第五代行動通訊系統、第六代行動通訊系統、輕量化協定、低軌道衛星

論文題目：利用對稱性及視角於條件式生成對抗網路之臉部補全方法

學校：高雄大學 資訊工程學系

研究生：吳金航

指導教授：洪宗貝

摘要：

臉部補全是影像補全的一個子領域，主要概念是利用與影像生成相關的演算法生成較自然且合理的內容填補人臉的缺失區域。臉部補全的應用相當廣泛，如人像照片毀損修補、去除物件遮擋復原人臉，人臉側臉轉為正臉等。臉部補全相較於一般的影像補全而言更具有挑戰性，因為必須考量到人臉的幾何結構與對稱屬性，以保證補全影像的合理性。在本論文中，我們提出了一種基於條件式生成對抗網路的兩階段臉部補全方法。在第一階段，我們訓練了一個基於深度學習的模型以預測人臉標記點，並在訓練時根據人臉在影像中的視角動態調整損失函數的懲罰值，以增強預測高視角人臉影像的能力。在第二階段，我們結合被遮擋的人臉影像與其對應的人臉標記點形成條件以訓練條件式生成對抗網路進行補全。如果輸入的遮擋影像接近正面臉，我們將在輸入模型之前對該影像進行對稱性處理。實驗結果顯示，我們在第一階段提出的訓練方法可以有效增強人臉標記點預測模型的穩健性，減少資料不平衡的影響，進而改善之後臉部補全的效果。此外，用我們在第二階段的方法訓練出來的臉部補全模型比之前相似架構的模型可以更好地保持補全人臉的幾何結構與對稱外觀。

關鍵字：條件式生成對抗網路、臉部補全、人臉標記點預測、對稱性處理

論文題目:根據非線性規劃及區間直覺模糊值之新的得分函數以作多屬性決策之新方法

學校：國立台灣科技大學 資訊工程系碩士班

研究生：鄧亨禮

指導教授：陳錫明

摘要：

本論文旨在根據非線性規劃法及我們所提之區間直覺模糊值之得分函數提出一個新的多屬性決策方法。首先，我們提出一個新的區間直覺模糊值之得分函數，以克服目前已存在之區間直覺模糊值之得分函數的缺點。然後，我們根據我們所提之區間直覺模糊值之得分函數計算決策者所提供的決策矩陣中之每一個區間直覺模糊值的得分值以建構轉換矩陣。然後，我們根據所得之轉換矩陣及決策者所給之每一個屬性的區間直覺模糊權重以建構一個非線性規劃模型。然後，我們求解此非線性規劃模型以得到每一個屬性的最佳權重。然後，我們根據所得到之轉換矩陣及所得到之每一個屬性的最佳權重計算每一個方案的加權得分。最後，我們根據每一個方案所得之加權得分對每一個方案進行排序。如果一個方案有較高之加權得分，則此方案具有更佳之偏好排序。我們所提之多屬性決策方法可以克服目前已存在之多屬性決策方法的缺點，其在區間直覺模糊值的環境中提供我們一個非常有用的方法以作多屬性決策。

關鍵字：決策矩陣、區間直覺模糊集合、區間直覺模糊值、多屬性決策、轉換矩陣、非線性規劃。

論文題目：根據區間直覺模糊值之新的得分函數及區間直覺模糊值之冪運算子以作多屬性決策之新方法

學校：國立台灣科技大學 資訊工程系 碩士班

研究生：游紹宏

指導教授：陳錫明

摘要：

本論文旨在根據我們所提之區間直覺模糊值之新的得分函數、區間直覺模糊值的冪運算子、及加權式決策矩陣提出一個新的多屬性決策方法。本論文所提出的區間直覺模糊值之新的得分函數是基於區間之 Beta 分佈的區間期望值所建構的，其可以克服目前已存在之區間直覺模糊值之得分函數的缺點。首先，我們根據所提之區間直覺模糊值之新的得分函數及每一個屬性之區間直覺模糊權重以計算得到每一個屬性的精確值權重，進而得到每一個屬性之正規化權重。然後，我們根據區間直覺模糊值之冪運算子、所得到之每一個屬性之正規化權重、及決策矩陣以建構加權式決策矩陣。然後，我們根據所得到之加權式決策矩陣及所提之區間直覺模糊值之新的得分函數以建構分數矩陣。然後，我們根據所得到之分數矩陣以計算每一個方案之得分。最後，我們根據所得到之每一個方案之得分以對每一個方案作排序。如果一個方案有較高之得分，則此方案具有更佳之偏好排序。我們所提之多屬性決策方法可以克服目前已存在之多屬性決策方法之缺點，其在區間直覺模糊值之環境中提供我們一個非常有用的方法以作多屬性決策。

關鍵字：區間直覺模糊集合、區間直覺模糊值、冪運算子、多屬性決策、得分函數、分數矩陣。