其他有利資料

1. 大學程式能力檢定(CPE)

臺灣程式競賽暨檢定學會
大學程式能力檢定

成　績　證　明

CPE 字第 2020100163 號

Collegiate Programming Examination
Association of Taiwan Computer Programming Contest
臺灣程式競賽暨檢定學會
大學程式能力檢定

邱歆惠（身分證字號：F230302793）
係國立中山大學資訊工程學系學生（學號：B083040031）
參與 2020 年 10 月 20 日程式能力檢定
特頒此狀　以茲證明

考試性質	3 小時，現場考試、封閉網路。考生不可攜帶文件資料進場。
解題數	4 題（共 7 題，全部平均解題數 1.09 題，最高解 7 題）
程式語言	C/C++
排名	47（排名比例：47/2180=2.2%）
發證日期	2022 年 9 月 28 日
等級	專業級：熟悉各種基礎的演算法、資料結構，並具有良好的程式編寫能力。

楊昌彪
臺灣程式競賽暨檢定學會 理事長

楊昌彪
大學程式能力檢定委員會 主席

2. 多益 ： 875 分

ETS TOEIC

CERTIFICATE OF ACHIEVEMENT

This is to certify that

CHIU SIN-HUEI

achieved the following scores on the

TOEIC® Listening & Reading Test

Listening	480
Reading	395
Total	875
as administered under the auspices of:	Chun Shin Limited
at:	Taiwan
date:	18-August-2022

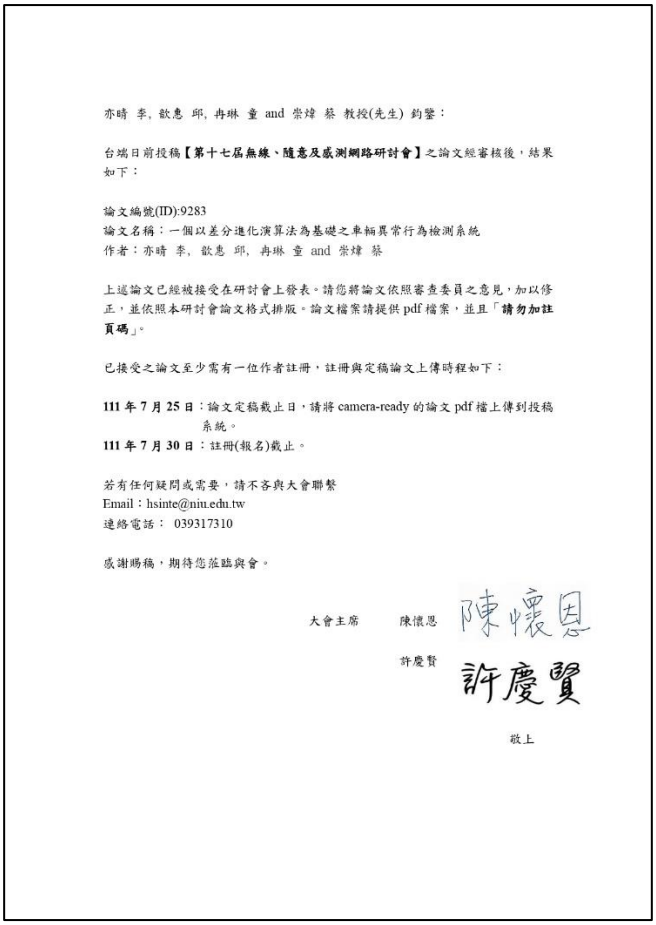
Updated TOEIC L&R
22072279

TOEIC SCALE

Joanna Gorin
Vice President
Global Language Learning Teaching & Assessment

ORIGINAL DOCUMENT HAS WATERMARK ON REVERSE SIDE

3. 第十七屆無線、隨意及感測網路研討會 ： 論文接受書



亦晴 李, 歆惠 邱, 冉琳 童 and 崇煒 蔡 教授(先生) 鈞鑒：

台端日前投稿【**第十七屆無線、隨意及感測網路研討會**】之論文經審核後，結果如下：

論文編號(ID):9283
論文名稱：一個以差分進化演算法為基礎之車輛異常行為檢測系統
作者：亦晴 李, 歆惠 邱, 冉琳 童 and 崇煒 蔡

上述論文已經被接受在研討會上發表。請您將論文依照審查委員之意見，加以修正，並依照本研討會論文格式排版。論文檔案請提供 pdf 檔案，並且「**請勿加註頁碼**」。

已接受之論文至少需有一位作者註冊，註冊與定稿論文上傳時程如下：

111 年 7 月 25 日：論文定稿截止日，請將 camera-ready 的論文 pdf 檔上傳到投稿系統。
111 年 7 月 30 日：註冊(報名)截止。

若有任何疑問或需要，請不吝與大會聯繫
Email：hsinte@niu.edu.tw
連絡電話： 039317310

感謝賜稿，期待您蒞臨與會。

大會主席 陳懷恩 陳懷恩
許慶賢 許慶賢

敬上

4. 第十七屆無線、隨意及感測網路研討會 ： 最佳論文獎

5. 論文(以下 7 頁)

一個以差分進化演算法為基礎之車輛異常行為檢測系統

李亦晴、邱歆惠、童冉琳、蔡崇煒
國立中山大學資訊工程學系
[xu3u42209, mavis1020039, lillian14261033]@gmail.com and cwtsai@cse.nsysu.edu.tw

摘要

車載隨意行動網路 (vehicular ad-hoc network; VANET) 可以支援車輛間以無線通訊交換訊息，以因應道路上的特殊狀況。VANET 作為網路系統始終存在受入侵風險，高準確度的車輛異常行為檢測系統 (misbehavior detection system; MDS) 是這之中非常重要的一個環節。許多現行 MDS 的需要以手動進行參數調整，存在效率不高的問題。本研究嘗試將 MDS 結合超參數自動最佳化，採用差分進化演算法 (differential evolution; DE) 進行策略性搜索近似最優解，針對不同異常行為分類器給予相應最佳化的超參數，並基於異常行為模式新增特徵，提升 MDS 辨識準確率。本研究以 VeReMi Extension 資料集做為訓練及評估的依據，相較未進行超參數最佳化的機器學習方法，本研究所提出的方法在四項評估異常車輛的辨識度指標中均有所提升，各項異常行為辨識準確率平均達近 98%，說明本研究所提出的方法為有效，能夠增加系統對異常行為的判斷準確率。

關鍵詞：VANET、車輛異常行為檢測系統、超參數最佳化、差分進化演算法。

Abstract

Vehicular ad-hoc network (VANET) enables vehicles to exchange road information by using wireless communication and helps the driver to decrease casualty risk when facing special traffic situations. As a network system, VANET has a high risk of cyber-attack, so that it is important to have high-accuracy misbehavior detection system (MDS). However, most of the recent works on MDS optimization adopt manual parameter tuning which is inefficient. In this paper, we focus on combining MDS with hyperparameter optimization, which uses differential evolution (DE) to make strategic selection and searches for optimal solutions. To make the detection more effective, optimized hyperparameters are given to the corresponding classifiers which was build based on different anomalous behavior. In addition, a new feature based on anomalous behavior is added to make the detection more effective. According to this study, the VeReMi extension dataset will be used to evaluate the performance of the proposed algorithm. The experiment indicates that the accuracy in detecting anomalous behavior is improved in four evaluation metrics. It can detect nearly 98% of anomaly vehicle trajectories in average. The result shows that the proposed method is more effective and can increase the detection of anomalous behavior.

Keywords: Vehicular ad-hoc network, misbehavior detection system, hyperparameter optimization, and differential evolution.

1. 前言

根據世界衛生組織於 2018 年提出的『Global status report on road safety 2018』[1] 指出，交通事故死亡人口逐年增長，並且於 2016 年在全球造成 135 萬人的喪生，在全年齡的死亡因素中排名第八，更在 5~29 歲年齡段中排名第一。交通事故所造成的損失並不僅止於生理上的損害，經濟合作暨發展組織 (organization for economic cooperation and development; OECD) 的研究 [2] 說明，交通事故造成的後續經濟與社會上成本的損失，在先進國家中佔其 GDP 的 2~5%，可見交通事故對人們影響之深遠。鑒於這些龐大損耗，各國對交通事故因應方式必須有所進展，除了由法律層面切入改進，科技也是可以著手輔助交通安全的方向，VANET 即是各國現在正在積極推展的研究之一，透過打造車輛對車輛 (vehicle-to-vehicle; V2V)、車輛對基礎設施 (vehicle-to-infrastructure; V2I) 相互溝通的網路，使道路上能有更充分的交流，對於交通安全、交通緩堵、自動駕駛等方面做出貢獻。VANET 的運行奠基於感測器蒐集車輛資訊，並藉由無線網路進行大量的資料交換與傳輸以利後續的判斷，能夠擴大且增強駕駛對於環境的感知力。但這種對資料正確度的依賴性，若任意環節遭遇故障，或遭受惡意攻擊等不可預估的錯誤時，可能對生命造成極大威脅。故障行為包括訊息延遲、速度或定位故障等所導致的資訊錯誤，而攻擊手法則包括阻斷服務攻擊 (denial of service; DoS) [3] 透過耗盡伺服器的資源或頻寬進而癱瘓網路。上述可能的故障及攻擊在本研究統稱為車輛的異常行為，這些異常行為儼然成為 VANET 中的一種危害。以車輛異常行為檢測系統為交換的訊息進行把關，是目前 VANET 環境中非常中需要發展的一個環節。

基本安全訊息 (basic safety message; BSM) 是由 SAE J2735 [4] 定義的訊息格式，包含車輛當前的位置、速度、加速度、方位等行車狀態，是車載 MDS 系統具體用以偵測是否異常的對象。車輛會透過定期低延遲的傳送 BSM 給周遭車輛，搭載於車載單元 (on board unit; OBU) 中的 MDS 即可對該車輛的訊息進行檢測。倘若分析結果為異常，OBU 會提醒鄰近車輛，並發送異常車輛的 Pseudo ID 給最近的路側單元 (road side unit; RSU) 以更新基地台資訊，並交由可信的第三方 (trusted third party; TTP) 對該異常車輛的憑證進行撤銷。過去研究中的檢測系統在判斷準確度上已有不錯的表現，但安全性問題需要更精確的判斷以排除潛藏危險。提升

判斷準確度的方法有很多，模型超參數最佳化是一個重要的研究議題，其主因爲現行許多機器學習系統以手動調整及測試模型超參數，不但較耗費人力及計算資源，最終結果仍可能失準且最佳化效率不高。近年來發展的自動化機器學習 (automated machine learning; AutoML) [5] 的概念可以彌補此缺陷，研究分支之一的超參數最佳化 (hyperparameter optimization; HPO) 是本論文採取的方式，透過機器學習方式自動嘗試、擇選最佳超參數設置以優化模型性能。同時也考量到 MDS 本身在大量資料訓練下的時間成本，選擇以超啟發式演算法中的差分進化演算法作為最佳化的驅動力，透過策略性的猜測，在合理的計算成本下找尋較佳解，以提升 MDS 分辨準確度。本文主要貢獻在於:

1) 透過超參數自動最佳化提升 MDS 模型檢測準確度。
2) 比較提出使用的差分進化演算法在不同分類器的最佳化成效。
3) 新增異常行為檢測特徵以提高模型檢測能力。

本文的行文脈絡如下: 第 2 節將分別回顧 VANET 中的入侵偵測系統與超參數最佳化研究的相關技術與發展，第 3 節將介紹系統的最佳化方法與實作，第 4 節則針對實驗結果進行分析與討論，第 5 節為結論。

2. 文獻探討

2.1 資料集

VANET 入侵偵測系統發展初期，主要由研究人員自行生成資料集，或使用模擬軟體作為評估系統的指標。因缺乏大型共通的參考性資料集，使得入侵偵測檢測機制間難以有相同指標比較性能優劣，使用模擬工具也會耗費相當複雜的步驟與高額成本。為解決此問題以促進相關研究的發展，Heijden 等人於 [6] 提出在以交通模擬軟體建立的盧森堡交通場景 (Luxembourg SUMO traffic; LuST) [7] 中，使用混和模擬框架 (vehicles in network simulation; VEINS) [8] 模擬車輛在 VANET 中的行為，藉此生成開源資料集 Vehicular Reference Misbehavior Dataset (VeReMi) ，資料集內容包含目標車輛所接收到鄰近車輛的 GPS 訊息與 BSM 作為測試資料。Kamel 在後續研究 [9]，以 VeReMi 資料集為基礎提出了 VeReMi Extension 資料集，修正原版本在異常行為 EventualStop 標記異常上較不合理的缺陷，新增異常行為種類，並在模擬中增加感測器誤差的模型，模仿實際情境中可能的位置、速度、加速度以及方向上的誤差，使資料集更貼近現實。

2.2 入侵偵測系統

早期入侵偵測系統主要以機器學習技術建構而成，像是 Grover 等人 [10] 提出使用集成學習，分辨以 NCTUns-5.0 模擬器 [11] 模擬 VANET 在不同場景中可能的車輛行為特徵，利用不同分類器的優勢，組合出比單一分類器更優秀的分辨能力，成功分辨車輛的異常行為。而在 VeReMi 資料集發表之後，針對 VANET 的異常行為檢測系統領域更是蓬勃發展，So 等人發表的論文 [12] 中，針對 VeReMi 資料集中位置欺騙的異常行為，在系統框架中提出了一套位置合理性檢查的特徵向量，並應用於 *K*-近鄰演算法 (*K*-nearest neighbors; KNN) 與支持向量機 (support vector machine; SVM) 模型，證實合理性檢查能夠為整體檢測準確度提升 20% 以上，並且該系統不僅能檢出 VANET 中的異常行為，還能對不同類型的已知異常行為進行分類，從而更具體且精準打擊異常行為。隨著深度學習相關研究逐漸豐厚，此技術也擴展應用至 VANET 的入侵偵測系統。Tejasvi 等人發表的研究 [13] 中，他們基於卷積神經網路 (convolutional neural network; CNN) 在序列分類中不需要人工提取特徵，且長短期記憶 (long short-term memory; LSTM) 在常見的時間序列的深度學習方法中，在較長的序列數據有較好表現的考量，選擇將 CNN 與 LSTM 結合用於重構位置模型，模型僅先以正常行為的數據進行訓練，在習得正常行為的模式後，若將異常行為數據輸入，基於模式產生重構的位置序列和輸入的序列會產生較大的誤差，最後透過閾值演算法計算誤差值分界，超過閾值者界定為異常，藉此達到分辨異常行為的目的，此研究也證實在重構模型上 CNN-LSTM 較單純堆疊式的 LSTM 擁有更好的性能。誠然重構階段的增加能夠為後續的判斷及分辨上帶來有利成效，可僅基於閾值即界定正常與異常可能有過於簡單、欠乏更多面向檢查的缺陷。基於上述考量，Cheng 等人發表的論文 [14] 提出了整合性算法的車載網路異常行為檢測系統，透過提取 [12] 使用的 SVM 分類方式，取代 [13] 方法中的閾值分類演算法，提出以深度學習 CNN-LSTM 方法進行位置重構，並使用 SVM 分類器進行異常行為的 MDS 系統架構，每個 SVM 分類器將考慮包括重構位置及合理性檢查在內的 11 個特徵，證實比起過去 [12] [13] 達到更佳的分辨率。

2.3 超參數最佳化

隨著機器學習被廣泛應用至各個領域而逐漸顯現，模型面臨必須適應不同情境的挑戰。超參數最佳化 (hyperparameter optimization; HPO) 的相關研究透過配置最適合的超參數組合，不僅能夠直接的提升模型性能，也有助於釐清對於特定問題適合使用的機器學習模型。藉由實現相同程度的超參數最佳化過程，使不同演算法建構的模型間更具比較性。主要流程如下 [15]:

1) 確立超參數最佳化的目標模型以及用以評估性能的指標，常見的評估指標包括準確度、均方根誤差 (root-mean-square error; RMSE) 等。
2) 總結該目標模型可調整的超參數組類型以確定適宜的最佳化方式。
3) 使用預設的超參數或常用值作為基準訓練模型。
4) 透過人工測試或對於問題領域既有認知，在大範圍的搜索空間鎖定可行解的範圍以開始最佳化 過程。
5) 根據當前測試性能良好的超參數值的區域縮小 搜索空間，或是在必要時探索新空間。
6) 在滿足結束條件時，返回性能最佳的超參數配置作為最終解。

選定適宜的最佳化方式是至關重要的一環，Li 等人 [16] 對於機器學習方面的 HPO 的統整性研究指出，許多 HPO 問題屬於非凸函數或具有不可微分特性，使得梯度下降等傳統最佳化演算法具有一定的限制性。其餘常用於最佳化超參數方法則是在不同使用情境下各有優劣，像是網格搜索 (grid search; GS) [17] 與隨機搜索 (random search; RS) [18]，研究中皆說明在足夠的

花費下，能夠找到全局最佳解或近似全局最佳解，但由於每次的嘗試間皆相互獨立，導致浪費大量時間搜索及評估表現不佳的區域，較適用搜索空間相對較小的情況。貝葉斯最佳化 (Bayesian optimization; BO) [19] 則能根據過去的測試結果決定未來的評估點，效率上高於 GS 與 RS，然而不同類型的 HPO 問題對於不同的代理模型的選擇具有限制。啟發式演算法 [20] 相對許多 HPO 方法複雜，但幾乎支援所有類型的超參數最佳化，在較大的搜索空間以及複雜的最佳化問題表現尤為出色，透過種群策略性地搜索，在相對少的迭代中也能獲得接近全局最佳解。Schmidt 等人 [21] 提出的研究實際比較上述方法，針對貝葉斯最佳化中基於序列模型的演算法架構 (sequential model-based algorithm configuration; SMAC)，與啟發式方法中的差分進化演算法 (differential evolution; DE) 進行超參數最佳化性能測試，實驗使用上述兩種方法最佳化包括 KNN、SVM、隨機森林等六種機器學習器的超參數，並以 49 個資料集的綜合表現作為評估，實驗結果表明 DE 最佳化模型超參數的性能在更多數的情況優於 SMAC，擁有更佳的泛用性。

3. 研究方法

本研究將以 Cheng 等人 [14] 所發表基於整合性演算法的車載 MDS 為基礎進行最佳化。鑒於該版本中對於所有異常行為的 SVM 分類器，在使用不同異常行為類型資料訓練的情況下皆採用相同的超參數，可能造成個別分類器無法達到最佳分辨成效的考量，本研究將針對不同異常行為類別的 SVM 分類器實作超參數最佳化，為不同分類器賦予最適合的超參數以提高最終的分辨成效。基於 Schmidt 等人 [21] 於論文中證實差分進化演算法在 HPO 問題上擁有更優異的表現，研究中將採用 DE 作為超參數最佳化的驅動力。作為一種啟發式演算法，以 DE 實作模型超參數最佳化同時能夠減少在 HPO 過程中，多次耗時模型訓練的時間成本，透過有策略性的猜測，使整個實作流程能夠控制在可以接受的花費下，更有效率的找尋近似的全局最佳解。

DE 演算法的核心概念仿照生物進化，透過種群中突變的個體與目標個體交配繁殖，不斷評選適應值高者存活。在突變環節的模擬，使用種群中隨機挑選兩個個體的向量差作為影響突變要素，以不同突變策略干擾待突變個體實現，產生的突變向量再和原先目標向量交叉組成子代，評比子代與目標向量的適應值，較佳者為新一代的目標向量，不斷循環直到條件終止。此概念運用在本研究針對 SVM 分類器的 HPO 架構如圖 1 表示，流程大致分作初始化、突變、交配、選擇，並檢查終止條件。不同向量代表的是不同的超參數組合，並且由於最佳化的目標是分辨異常行為的 SVM 分類器，研究採用交叉驗證下準確度的平均為個體評估適應值，終止條件則是以產生的世代數量為限，若條件終止則最後的種群最佳解，即是透過 DE 得出對於該車輛異常行為 SVM 分類器的最佳超參數組合。總體來說 HPO 可以提升固有 SVM 分類器在異常行為分辨的準確度，那麼透過提升原始分類器的判斷能力，以此更好的基礎作為超參數最佳化的對象，應能更大幅的提升整體效能，本研究基於以上考量，另外也針對原先判斷準確度較差的異常行為類別，依據異常行為模式增加判斷特徵，提升整體判斷力以達成更佳成效。

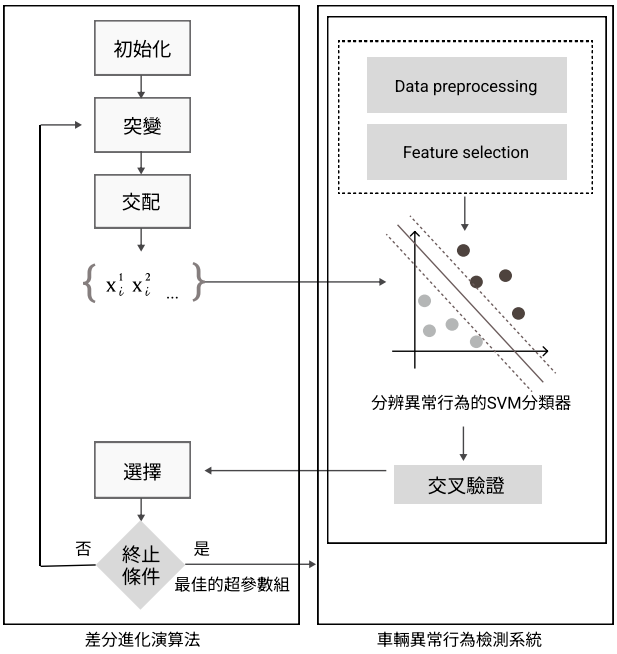


圖 1: 以 DE 實現車載 MDS 超參數最佳化架構

3.1 以 DE 實作 HPO 各項程序

本節將詳述針對圖 1 架構中各項具體實現細節，鑒於原系統採用 SVM 分類器分辨是否為異常行為，本節 HPO 流程主要以 SVM 設定為例，表 1 所示即在不同 kernel 下可調整的超參數組合。在初步的研究測試中，考量不同 kernel 之間核函數參數 γ 計算方式的不同，較不適宜相互繼承運算，並且 RBF 在測試中的表現優於其他 kernel，本研究主要基於 RBF kernel 下調整 C 及 γ 的組合達成最佳化模型目的。

表 1: SVM 分類器可調整之超參數

kernel	hyperparameter
RBF	C, γ
Poly	C, γ ,degree,coef0
sigmoid	C, γ ,coef0

懲罰係數 C 控制的是對於誤差的寬容度，用於平衡分類的錯誤率與支持向量複雜度，當 C 愈大則愈不容許誤差存在，表示會將較遠的離群點納入考量，支持向量增多則模型也隨之變得複雜，若設定過大容易造成擬合過度。另一超參數是核函數參數 γ，此超參數左右的是支持向量的影響範圍，和影響半徑呈倒數關係，若 γ 愈小則單一支持向量影響範圍愈大，設定過小導致模型較難以捕捉較精細或複雜的模式。本研究透過調整 C 及 γ 的值，使模型能夠平衡於適宜的複雜度，對於異常行為有恰當的判斷。

A. 初始化

初始化步驟在於隨機產生大小為 $n_{\|p\|}$ 的初始種群，每個個體 x_i 向量編碼由最佳化目標超參數構成，公式如下:

$$x_i = (x_i^1, x_i^2, ..., x_i^d). \tag{1}$$

本論文主要以 SVM 為例，調整超參數 C 及 γ 的值，故維度 $d=2$，且 x_i^1 所代表的是懲罰係數 C，而 x_i^2 則是核函數參數 γ。一般期望初始種群能夠均勻覆蓋全部區域，以更充分搜尋全域最佳解，各個個體產生方式是對於各維度在範圍內隨機產生值組成，各維度由於表述不同的超參數，所以範圍定義各不相同，通常採用人工測試或對於問題領域既有認知界定上下界。具體公式(2)如下:

$$x_{i,0}^j = x_{\min}^j + \text{rand}(0,1)\times(x_{\max}^j - x_{\min}^j), \tag{2}$$

$x_{\max}^j$ 及 $x_{\min}^j$ 分別為設定的第 j 維度的上下界，而 $i = \{1,2,\ldots,n_{\|p\|}\}$。

B. 突變

接著執行差分突變操作產生突變向量 $v_{i,t+1}$，以產生既有種群外的超參數組合。DE 在模擬突變上具有許多不同策略，核心概念都是透過隨機挑選種群中的向量差，乘上突變權重 F 等相關操作構成突變向量。本研究中採用的突變策略是 DE/rand-to-best/1，同時考量當前種群最佳超參數組及隨機組合，兼顧策略性猜測也防止過早收斂，公式如下:

$$v_{i,t+1} = x_{r1,t} + (x_{\text{best},t} - x_{r1,t}) + F\times(x_{r2,t} - x_{r3,t}), \tag{3}$$

$r1、r2、r3 \in \{1,2,\ldots,n_{\|p\|}\}$，且 $r1 \neq r2 \neq r3$，t 所表示的是當前迭代次數。另外在 F 作為 DE 的控制參數之一，由於具有過大則突變擾動度大、不易收斂，過小可能收斂過早，落入區域最佳解的特性，為了使迭代前期能夠適度保有探索多樣性，而後期能夠更多考量種群最佳解加快收斂，本研究在 F 的設定上，額外納入模擬退火演算法 (simulation annealing; SA) 的降溫機制，透過逐次迭代下不斷縮小 F 值達成以上目的。

C. 交配

此步驟目的是使目標向量 $x_{i,t}$ 與突變向量 $v_{i,t+1}$ 交叉產生新子代的超參數組，此新子代又稱作試驗向量 $u_{i,t+1}$，決定此步驟的關鍵因子是雜交概率 c_r，假設亂數產生之值大於 c_r，則新子代保留原目標向量該維之超參數值；反之則選用突變向量值。另外為確保子代及父代組合不同，以免失去比較性，會至少選定一個維度的超參數 j_{rand} 不受機率影響必定更改，本研究中則表示新子代的超參數組 C 與 γ 之間，必定至少有其一接受突變向量產生的新值，公式如下:

$$u_{i,G+1}^j = \begin{cases} v_{i,t+1}^j & \text{if rand}_{j[0,1)} \leq c_r \text{ or } j = j_{\text{rand}}, \\ x_{i,t}^j & \text{other.} \end{cases} \tag{4}$$

D. 選擇

產生新子代後，接著要對試驗向量與目標向量進行比較，選擇留下子代或是父代。又因本研究應用的情境是分辨是否為異常行為，採用 k 折交叉驗證將訓練集分組，每次將 $k-1$ 組作為訓練集訓練模型，剩餘一組作為驗證集評估該模型訓練的準確度，取平均值作為評比標準，較高者留下作為新一代的目標向量。公式如下:

$$x_{i,t+1} = \begin{cases} u_{i,t+1} & \text{if } f(u_{i,t+1}) \geq f(x_{i,t}), \\ x_{i,t} & \text{other.} \end{cases} \tag{5}$$

其中 $f()$ 輸入為試驗向量或目標向量的超參數組，以該組合訓練模型進行 k 折交叉驗證，並對多次驗證的準確度計算平均值作為輸出。

此步驟後若仍不滿足終止條件則回到突變步驟持續產生下一代新的超參數組合，反之若達最大迭代數或連續 10 代在 k 折交叉驗證結果都未能勝過父代，則立即終止並輸出當前最佳解，作為該車輛異常行為分類器的最佳超參數組合。

3.2 特徵

除了透過 HPO 過程提升模型效能，也能依照個別異常行為特性標記新特徵，提升某些現階段仍舊較難以分辨是否異常的行為。像是 EventualStop 的異常行為類別，此類別具體異常行為體現於凍結位置並將速度值設為空，模擬車輛突發異常靜止的攻擊型態，則依此定義敘述可擴展成以下式子辨認是否為此類異常行為:

$$k_i = \begin{cases} K & \text{if } s_{i-1}(v) \neq 0 \wedge s_{i-1}(x,y) = s_i(x,y), \\ 0 & \text{other.} \end{cases} \tag{6}$$

若單台車輛的時間序列訊息中，在前一刻的速度訊息不為 0、仍舊處在移動的情況下，此刻位置卻與前一時刻相同，則視作異常行為並標記特徵為 K 值，反之設為 0。將此序列標記作為第 12 種特徵輸入 SVM 分類器，以提升對於該異常行為類別的判斷力。

4. 結果與討論

4.1 資料集與 MDS 重建

本研究將重建 Cheng 等人 [14] 發表的車輛異常行為檢測系統，並使用 VeReMi extension 資料集 [9] 進行模型訓練與評估。

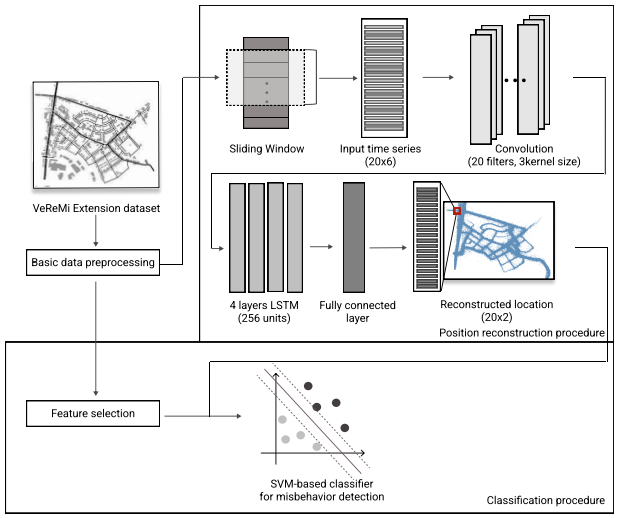


圖 2: 車載 MDS 架構

資料集中包含正常及 19 種車輛異常行為的 BSM，內容囊括輛車輛的位置、速度、加速度、發送時間等狀態，研究中將資料集分批用於圖2中系統建立的兩個階

段。位置重構階段以 CNN-LSTM 模型生成特徵，表示被檢測車輛的行為與標準行為模式的差異。模型訓練以 90% 的正常行為時間序列做為輸入，建立標準行為模式，輸入向量包括 x、y 軸上的位置、速度及加速度共計 6 項資訊，以 20 個向量為單位構成一個時間序列，並設定大小為 10 的滑動窗口，每次將與前次重疊 10 組向量，生成用於訓練模型的時間序列數據。訓練好的重構模型可以基於正常行為模式預測車輛位置，倘若輸入為異常行為數據，則預測出的位置將會與資料位置產生較大誤差，此誤差可作為下階段的輸入特徵之一，與使用剩餘資料的 70% 所生成的特徵共同訓練 SVM 分類器，細節如表2。

表 2: SVM 分類器於本研究之 11 項輸入特徵

	特徵	說明
1	行為偏差	車輛行為與標準模式間的偏差
2	位置合理性檢查	以位移方程式測試位移區間合理性
3	速度資訊	以總位移和時間計算平均速度 (x 軸)
4	速度資訊	以速度和時間預測平均速度 (x 軸)
5	速度資訊	特徵 3 與特徵 4 的差異
6	速度資訊	以總位移和時間計算平均速度 (y 軸)
7	速度資訊	以速度和時間預測平均速度 (y 軸)
8	速度資訊	特徵 6 與特徵 7 的差異
9	距離資訊	透過每兩個 BSM 位置計算總距離
10	距離資訊	以平均速度預測總位移
11	距離資訊	特徵 9 與特徵 10 的差異

在分類階段中，則是運用 11 項特徵分別訓練針對不同異常行為的 SVM 分類器，並使用剩餘資料的 30% 作為測試集，評估對於 19 種不同異常行為分辨成效。

4.2 實驗設定與分析

本研究的實驗聚焦於針對分類階段的模型進行以 DE 驅動的超參數最佳化，並進行一系列比較。實驗一比較重建的原始系統與經 HPO 過程後對異常行為分辨準確度差異，以證實提出的 DE 在最佳化模型超參數上為有效。實驗二透過比較不同分類器經 HPO 過程的成效，觀察此方法對於不同模型的適用性。實驗三則比較原始與新增本研究提出之特徵的系統，同樣經 HPO 過程後的差異性，以驗證新增的特徵能夠提升對於異常行為的判定能力。

A. 實驗一 使用 SVM 分類並進行超參數最佳化

本實驗將針對重建的 MDS 中 SVM 分類器，實現研究中以 DE 驅動的 HPO 流程，參數設定如表3。由於最佳化目標 SVM 分類器僅需調整懲罰參數 C 及核函數參數 γ，在搜索空間相對較小的情況下，初始種群規模 $n_{\|p\|}$ 也相對設定較小。初始化階段在設定的超參數值上下界內，隨機產生 7 組超參數組合作為初始種群，在突變階段參考突變權重 F 產生種群外的組合，且 F 值將會因迭代次數的增加而成比例減少。交配階段則大致由概率 c_r 決定目標向量的置換率，最後在選擇階段中留下子代與父代中評價較高者，並且若達最大迭代數或在連續數代都未見發展性，則立即終止並輸出當前最佳解，作為該車輛異常行為分類器的最佳超參數組合實驗一結果如圖3，比較原始系統與經 HPO 過程的系統分別在 19 種異常行為分辨準確度，多數分類器對異常行為判斷的準確度皆近於 100%，而在如 ConstPosOffset、EventualStop 原始分辨準度較低者，則可見

表 3: 參數設定

C	0.5~2	γ	0.01~0.5
$n_{\|p\|}$	7	F	0.8
c_r	0.75	max_generation	200

經最佳化過程後較顯著的提升，其中又以 ConstPosOffset 以 2.4% 為最高的提升度，在四項指標準確度 (Accuracy)、精確度 (Precision)、召回率 (Recall) 及 F1-score 評估下，所有異常行為分辨平均上有 0.3%~0.7% 成長，由此可證實提出的 DE 在最佳化模型超參數上具有一定成效。

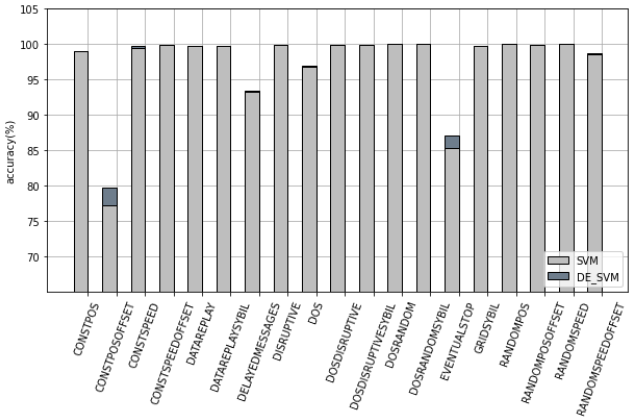


圖 3: 經 HPO 之 SVM 分類器於 19 種異常行為分辨成效

B. 實驗二 使用 DE 進行其他分類器之超參數最佳化

研究中同時嘗試 SVM 外的 3 種分類器經 HPO 過程後的成效，以觀測此方法在不同分類器上的適用性。實驗對象包括 KNN、Decision tree、XGBoost，分類器可調整的超參數選項如表4。

表 4: 各分類器可調整之超參數

classifier	hyperparameter
KNN	n_neighbors, p, weights
Decision Tree	criterion, splitter, max_depth, class_weight, min_samples_split, min_samples_leaf, max_features
XGBoost	objective, eval_metric, max_depth, eta, min_child_weigt, γ, subsample, colsample_bytree

KNN 主要透過調整鄰居數量與距離計算方式最佳化模型，而 Decision tree 會修改各個節點的最小訓練樣本數，同時考慮樹的最大深度與分枝時參考的特徵數，調整 criterion 參數去尋找最佳節點與分枝，XGBoost 則是固定使用 gbtree booster 並操控此 booster 的相關參數如 eta、γ 等，調整每次分類的權重與損失函數下降幅度，以及如 Decision tree 一樣控制分類樹相關參數，最後挑選損失函數與評估指標的類型以最佳化模型。實驗比較不同分類器分別以設定預設值的模型與經 HPO 流程調整參數的模型分辨異常行為，以準確度的差異性作為此方法對於不同分類器適用性的比較基準。

實驗二結果如圖4、5所示，上方黑色區塊所代表的是對於該異常行為分辨準確度的提升率。由圖可觀察在各分類器皆屬預設參數值的情況下，SVM 相較於其他分類器擁有更高的平均準確度，而經過以 DE 最

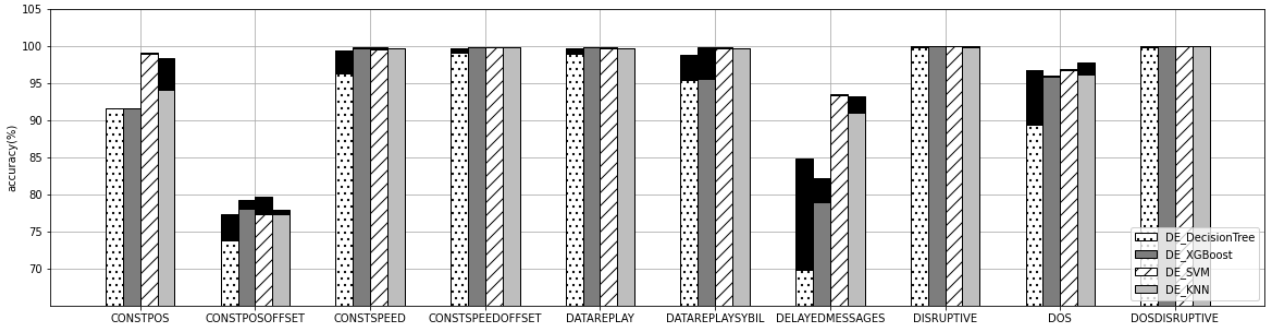


圖 4: 不同分類器經 HPO 流程於 19 種異常行為分辨成效比較-1

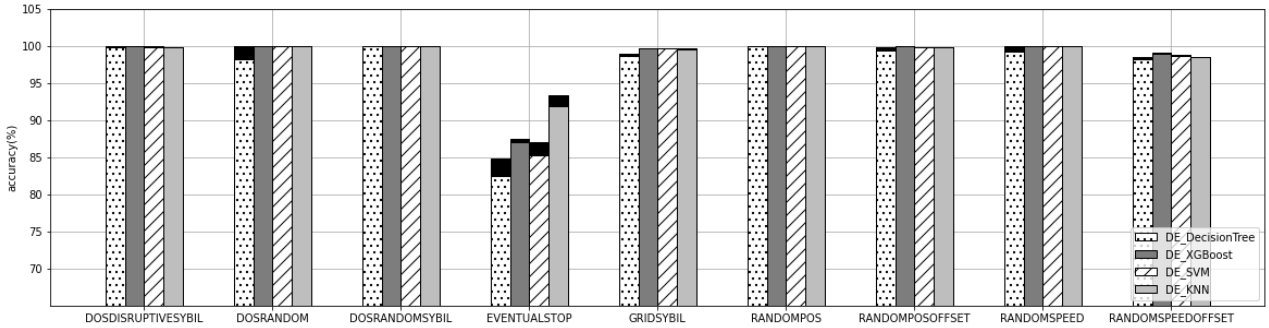


圖 5: 不同分類器經 HPO 流程於 19 種異常行為分辨成效比較-2

佳化模型超參數組合的處理後，各分類器在預設狀態下判斷力較低的異常行為類別都有相對顯著的提升，其中 KNN 對於異常行為類別 ConstPost 的分辨度有最高的 4.2% 提升，而 XGBoost 在 DatareplaySybil 的異常行為類別上有最高的 4.1% 準確率提升，Decision tree 則是在 DelayedMessages 的異常行為類別上擁有最高的 13% 準確率提升，整體平均上各分類器分辨率皆有成長，以 KNN 在所有異常行為的分辨平均升高準確率 0.56%，使用 F1-score 進行評估也能有 0.65% 的提升。總體而言，本研究所使用的方法應用於此車載 MDS 的超參數最佳化情境中，對於 KNN 分類器在平均上有更佳的成長率，並且對於列舉的分類器皆能有不同程度的有效提升。

C. 實驗三 使用新特徵並進行超參數最佳化

實驗三比較以重建的系統進行 HPO 流程與使用新特徵並進行 HPO 流程，在各異常行為分辨準確度的差異。

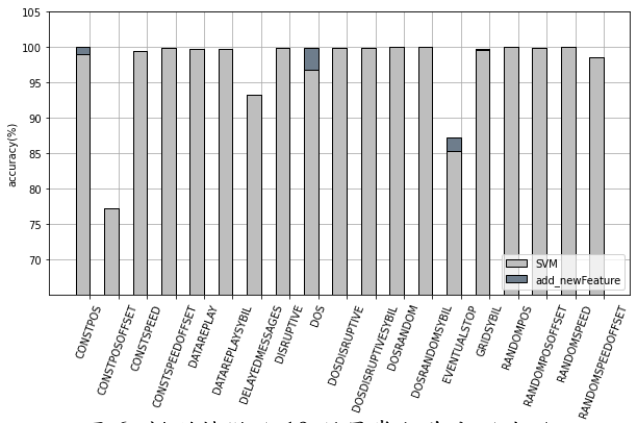


圖 6: 新增特徵於 19 種異常行為分辨成效

實驗結果如圖6，可以觀察到在異常行為類別 ConstPost、DoS、EventualStop 三者提升較多，以在 DoS 類別準確率 (Accuracy) 提升 3.2% 為最高，並且三者在精確度 (Precision) 的提升相較準確度更為顯著，在 DoS 類別平均提升 4.2%、EventualStop 類別則平均提升 3.5% 的精確度，表示新增的特徵更傾向於透過減少對於正常行為被誤判為異常的情況，提升整體判斷能力。

5. 結論與未來工作

本研究透過提出的 DE 演算法驅動的模型超參數最佳化，同時增加基於 EventualStop 異常行為模式啟發生成的特徵，提升模型對於是否為異常行為判斷力。本論文以三項實驗橫向比較論證以上方法有效，實驗一比較重建的 MDS [14] 與經 HPO 過程最佳化的 MDS 對於 19 種異常行為的判斷準確度差異，實驗結果表明在原分辨率較低的異常行為最多能提升平均 2.4% 準確度，證實此方法能夠成功提升模型效能；實驗二對比 SVM、KNN、Decision tree 及 XGBoost 四種分類器在預設超參數值與經超參數最佳化的情況下，對於 19 種異常行為判斷準確度變化程度，實驗可知以 KNN 平均提升度最為顯著，並且對於上述分類器皆有不同程度的有效提升；實驗三則比較使用新特徵前後差異，在 ConstPost、DoS、EventualStop 三項異常行為上有較顯著提升，驗證新特徵對於模型在異常行為的判斷上為有效，最終實驗結果說明使用本研究中以 DE 演算法驅動的 HPO，與增加基於 EventualStop 異常行為模式生成的新特徵，能夠使車輛異常行為檢測系統達到平均 97.6% 的分辨準確率。

誌謝

本研究由科技部大專學生研究計畫補助，計畫編號 MOST 111-2813-C-110-031-E，科技部專題計畫補助，計畫編號 MOST108-2221-E-005-021-MY3，特此致謝。

參考文獻

[1] W. H. Organization, "Global status report on road safety 2018," 2018. [Online]. Available: https://www.who.int/publications/i/item/9789241565684

[2] I. T. Forum, "Zero road deaths and serious injuries," 2016. [Online]. Available: https://www.oecd-ilibrary.org/content/publication/9789282108055-en

[3] H. Hasbullah and I. A. Soomro, "Denial of service (DOS) attack and its possible solutions in VANET," *International Journal of Electronics and Communication Engineering*, vol. 4, no. 5, pp. 813–817, 2010.

[4] B. E. Roy Sumner and J. Baker, "SAE J2735 standard: Applying the systems engineering process," 2013. [Online]. Available: https://rosap.ntl.bts.gov/view/dot/3413

[5] X. He, K. Zhao, and X. Chu, "AutoML: A survey of the state-of-the-art," *Knowledge-Based Systems*, vol. 212, p. 106622, 2021.

[6] R. W. Heijden, T. Lukaseder, and F. Kargl, "VeReMi: A dataset for comparable evaluation of misbehavior detection in VANETs," in *Proceedings of the International Conference on Security and Privacy in Communication Systems*, 2018, pp. 318–337.

[7] L. Codecá, R. Frank, S. Faye, and T. Engel, "Luxembourg SUMO traffic (LuST) scenario: Traffic demand evaluation," *IEEE Intelligent Transportation Systems Magazine*, vol. 9, no. 2, pp. 52–63, 2017.

[8] C. Sommer, R. German, and F. Dressler, "Bidirectionally coupled network and road traffic simulation for improved IVC analysis," *IEEE Transactions on Mobile Computing*, vol. 10, no. 1, pp. 3–15, 2010.

[9] J. Kamel, M. Wolf, R. W. van der Hei, A. Kaiser, P. Urien, and F. Kargl, "VeReMi extension: A dataset for comparable evaluation of misbehavior detection in VANETs," in *Proceedings of the ICC 2020-2020 IEEE International Conference on Communications*, 2020, pp. 1–6.

[10] J. Grover, V. Laxmi, and M. S. Gaur, "Misbehavior detection based on ensemble learning in VANETs," in *Proceedings of the International Conference on Advanced Computing, Networking and Security*, 2011, pp. 602–611.

[11] S.-Y. Wang and C. Chou, "NCTUns 5.0 network simulator for advanced wireless vehicular network researches," in *Proceedings of the 2009 Tenth International Conference on Mobile Data Management: Systems, Services and Middleware*, 2009, pp. 375–376.

[12] S. So, P. Sharma, and J. Petit, "Integrating plausibility checks and machine learning for misbehavior detection in VANET," in *Proceedings of the 2018 17th IEEE International Conference on Machine Learning and Applications*, 2018, pp. 564–571.

[13] T. Alladi, A. Agrawal, B. Gera, V. Chamola, B. Sikdar, and M. Guizani, "Deep neural networks for securing IoT enabled vehicular ad-hoc networks," in *Proceedings of the ICC 2021-IEEE International Conference on Communications*, 2021, pp. 1–6.

[14] H.-Y. Hsu, N.-H. Cheng, and C.-W. Tsai, "A deep learning-based integrated algorithm for misbehavior detection system in VANETs," in *Proceedings of the 2021 ACM International Conference on Intelligent Computing and its Emerging Applications*, 2021, pp. 53–58.

[15] G. Luo, "A review of automatic selection methods for machine learning algorithms and hyper-parameter values," *Network Modeling Analysis in Health Informatics and Bioinformatics*, vol. 5, no. 1, pp. 1–16, 2016.

[16] L. Yang and A. Shami, "On hyperparameter optimization of machine learning algorithms: Theory and practice," *Neurocomputing*, vol. 415, pp. 295–316, 2020.

[17] M. Injadat, A. Moubayed, A. B. Nassif, and A. Shami, "Systematic ensemble model selection approach for educational data mining," *Knowledge-Based Systems*, vol. 200, p. 105992, 2020.

[18] J. Bergstra and Y. Bengio, "Random search for hyper-parameter optimization," *Journal of Machine Learning Research*, vol. 13, 2012.

[19] J. Snoek, H. Larochelle, and R. P. Adams, "Practical bayesian optimization of machine learning algorithms," *Advances in Neural Information Processing Systems*, vol. 25, no. 2, 2012.

[20] A. Gogna and A. Tayal, "Metaheuristics: Review and application," *Journal of Experimental & Theoretical Artificial Intelligence*, vol. 25, no. 4, pp. 503–526, 2013.

[21] M. Schmidt, S. Safarani, J. Gastinger, T. Jacobs, S. Nicolas, and A. Schülke, "On the performance of differential evolution for hyperparameter tuning," in *Proceedings of the 2019 International Joint Conference on Neural Networks*, 2019, pp. 1–8.