基於 UN R155 安全指標的車輛網絡攻擊測試設計與實施

袁梓曛 [1]、黃胤凱 [1]、王科元 [1]、王郁翔 [2]、許富皓 [3]、劉耀中 [4]、林庭佑 [4]

[1] 國立中央大學資訊工程學系(學士生)

[2] 國立中央大學資訊工程學系(碩士生)

[3] 國立中央大學資訊工程學系(教授)

[4] 財團法人車輛測試研究中心(研究員)

E-mail*: kev900102in@gmail.com

計畫編號: 11314026

摘要

隨著車聯網技術的發展，車輛的資訊安全已成為全球關注的重點。聯合國經濟委員會 (United Nations Economic Commission for Europe, UNECE) 於 2021 年發布了關於車輛資訊安全的法規—— UN Regulation No. 155 (UN R155)，為車輛製造商及供應商提供了詳細的資訊安全合規要求 [1]。然而，對於這些規範的實際落實與測試，特別是這種攻擊向量與路徑的驗證，仍有待進一步探討。本研究旨在依據 UN R155 所列的安全性指標[5]， 設計並實作以車聯網系統為目標的攻擊測試腳本。透過模擬各種潛在的攻擊場景，如惡意軟體植入、網路中間人攻擊及系統漏洞利用，來檢測車輛系統的防禦能力與應對機制[9][15][16]。本文將詳細介紹攻擊腳本的開發過程、測試環境的設置以及針對部分指標的測試結果，並根據結果提供系統防禦的解決方案。研究結果不僅能證明 UN R155 的可部屬性，亦能為車輛製造商驗證資訊安全解決方案的有效性，以進一步提升整體車聯網安全水平。

關鍵詞：資訊安全，攻擊測試，車聯網。

1. 前言

隨著車輛自動化、電動化以及車聯網技術（Vehicle-to-Everything, V2X）的快速發展 [10][18]，現代汽車已不再僅僅是一種交通工具，而成為一個複雜的網路終端。車輛內部的電控單元（Electronic Control Units, ECU）、通信模組、感測器與外部網路相連，使車輛能夠進行高效的數據交換與即時通信，從而提升駕駛體驗與安全性 [3][11]。然而，這些技術的引入也使車輛暴露在更大的資訊安全風險之中[4]。駭客可以透過車載網路入侵系統，篡改關鍵數據或直接控制車輛，從而對車輛的安全、乘客隱私以及整體交通系統帶來潛在危害。

為了應對這些日益嚴峻的安全挑戰，聯合國經濟委員會（UNECE）於 2021 年發布了 UN R155《車輛網路安全法規》，該法規要求車輛製造商在車輛生命週期內建立健全的網路安全管理系統（CSMS），並對產品進行持續的風險評估、漏洞管理及安全防護措施的更新[5][9]。UN R155 明確提出了一系列關鍵指標，以指導汽車業界在設計、開發、測試和部署車輛時，如何確保系統的網路安全[8] [17]。然而，這些規範的具體實施與測試標準在不同車輛系統中的應用效果，仍然需要通過實際的攻擊模擬來驗證[1]。

本研究旨在針對 UN R155 所列的各項指標，設計並實作一套攻擊測試腳本，用以模擬真實的攻擊場景，評估車聯網系統在各類攻擊情境下的防禦能力。在其中我們

實作出了 UN R155 部分攻擊，並將其系統化的整合，其中包含以下:

一、 對後端伺服器的攻擊導致後端伺服器停止運行的攻擊，例如，阻斷後端伺服器讓車輛無法互動[14]，對應於 UN R155 第 2.1 條款。

二、 針對更新伺服器或網路的拒絕服務攻擊，以阻止關鍵軟體更新的推出和/或解鎖客戶特定功能，對應於 UN R155 第 13.1 條款

三、 針對多餘服務的網路連接埠是否為開啟狀態，而導致不信任的外部網路能連接存取，對應於 UN R155 第 29.1 條款。

四、 檢查車輛系統是否會接收不可靠或不可信來源的訊息，對應於 UN R155 第 6.1 條款。

五、 對車輛通訊系統發送欺騙訊息，例如 802.11p 的 V2X、GNSS 訊息等[12][13]，對應於 UN R155 第 4.1 條款。

六、 重播攻擊，例如針對通訊網關的攻擊允許攻擊者降級 ECU 的軟體或網關的韌體，對應於 UN R155 第 6.3 條款。

七、 向車輛通訊系統發送大量垃圾數據，導致車輛資訊系統無法正常提供服務，對應於 UN R155 第 8.1 條款。

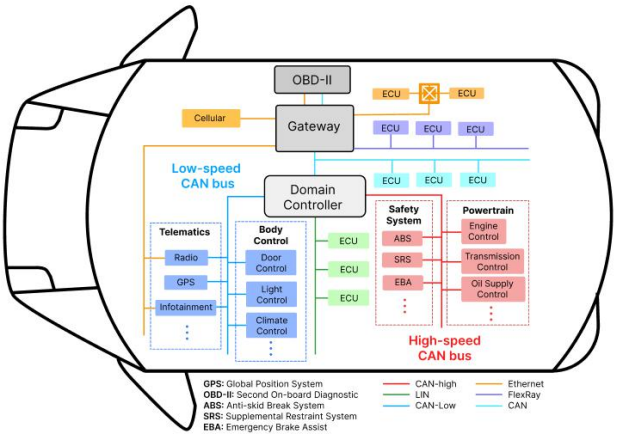
本研究的貢獻在於不僅驗證了 UN R155 規範的可操作性和實際效用，還提供了針對車聯網系統進行安全測試的標準化流程[5][21]。透過攻擊腳本的測試結果，製造商可以更全面地了解其產品的潛在弱點，進而根據實際威脅制定更具針對性的防護措施，從而提升整體車輛網路安全水平。隨著汽車產業逐步邁向智慧化與連接化，強化車輛資訊安全將成為保障未來交通安全與穩定運行的關鍵[11]。

1.1 核心通信協議

不同的通信協議在汽車內部應用，如圖一，針對不同的功能需求，提供了各自的優勢：

- Controller Area Network (CAN)是汽車中最廣泛使用的通信協議，適用於實時要求較高的系統，如發動機控制、煞車和變速箱。它以高可靠性和抗干擾能力著稱，支持多個 ECUs 之間的數據傳輸。
- Local Interconnect Network (LIN)是一種低速、低成本的通信協議，通常用於車內非關鍵功能的控制，如車窗、座椅調節和空調系統。LIN 一般與 CAN 協同工作，用於減少總線負載。
- Media Oriented Systems Transport (MOST)是一種高速多媒體數據傳輸協議，專為信息娛樂系統設計，支持高帶寬的音頻和視頻數據傳輸。
- FlexRay 提供高帶寬和冗餘特性，適用於需要精確控制和高可靠性的應用，如自動駕駛輔助系統（ADAS）和底盤控制系統。相比 CAN，FlexRay 具有更高的數據傳輸速率和更強的容錯能力。

隨著車輛自動化技術的發展，汽車乙太網路(Automotive Ethernet)逐漸成為下一代汽車通信架構的重要部分。它支持更高的數據傳輸速率（高達 1 Gbps），非常適合處理自動駕駛、ADAS 以及車輛與外部基礎設施的通信需求（如 V2X 通信）。



圖一、車輛內部網路示意圖

1.2 汽車通信架構的分層

汽車通信架構通常採用分層的設計，這些層次構成了整車通信系統的基本結構：

1. 感知層：負責收集車輛周圍環境的信息，如雷達、攝像頭和各類傳感器，將數據傳遞至控制單元。
2. 網絡層：包括各種車內通信協議，如 CAN、LIN、MOST、FlexRay 和乙太網等，用於確保數據能夠在不同的 ECUs 之間高效傳輸。
3. 應用層：是直接與駕駛者或其他車輛功能交互的層次，處理如車輛控制、信息娛樂、導航等應用，並確保不同系統間的協同運作。

1.3 Controller Area Network

CAN 以其獨特的技術特性而聞名，這些特性使其在高噪聲環境中進行實時、可靠的數據通信成為可能。以下是 CAN 協議的一些重要技術特性，這些特性確保了其在嵌入式系統中的廣泛應用[15][16][23]。

1.3.1 多主機架構

CAN 使用的是一種多主機 （multi-master）架構，這意味著連接到 CAN 總線的任何 ECU 都可以在總線空閒時主動發送訊息，無需中央控制器或主節點來管理通信。這使得每個設備都有機會在需要時發起通信，從而增強了系統的靈活性和容錯性。

1.3.2 CSMA/CD 與優先級仲裁

CAN 採用了載波監聽多路訪問/碰撞檢測（CSMA/CD）技術來管理總線上的通信。這種技術確保了當多個節點嘗試同時發送數據時，系統可以通過檢測沖突來進行仲裁。CAN 的仲裁過程是基於訊息識別碼的優先級仲裁機制：當發生碰撞時，優先級較高的訊息（識別碼數值較小）可以繼續傳輸，優先級較低的節點則會等待下次發送機會。這種設計確保了關鍵數據能夠即時傳輸，特別是在車輛安全相關的應用中。

1.3.3 差分信號傳輸與抗干擾能力

CAN 使用差分信號（differential signaling）進行通信，通過兩條總線線路（CAN_H 和 CAN_L）同時傳輸信號的正負電位來表示數據。這種技術極大提高了 CAN 總線的抗干擾能力，因為外部的電磁干擾對兩條總線會產生相同的影響，從而被抵消。此外，差分信號還有助於延長通信距離並提高傳輸的可靠性，這對於汽車和工業環境中的高噪聲環境至關重要。

1.3.4 錯誤檢測與錯誤處理機制

CAN 可以檢測多種錯誤，包括位錯誤、填充錯誤、CRC 錯誤、格式錯誤和 ACK 錯誤。每個節點在發送訊息時會持續監控總線狀態，若發現錯誤，該節點會立即停止發送並重試。CAN 還引入了錯誤計數器，當某節點的錯誤數量超過預定閾值時，該節點會被暫時隔離，防止其繼續發送錯誤數據，這保證了總線的整體通信質量。

1.3.5 高效通信下的訊息識別

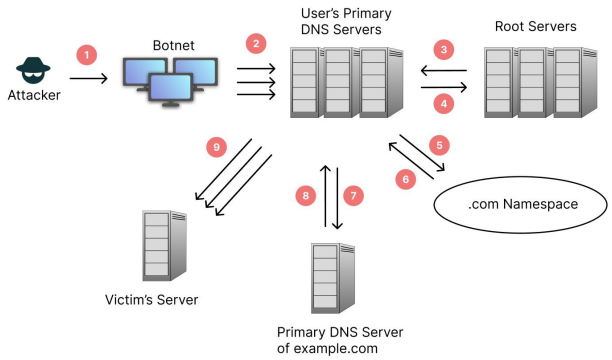
CAN（Controller Area Network）協議是一種基於訊息識別碼（ID）的通信協議，廣泛應用於車輛電子控制單元（ECUs）之間的數據傳輸。通過識別碼進行優先級仲裁和訊息過濾，確保優先級較高的數據優先傳輸，提升網絡實時性。 CAN 採用非返回零位編碼（NRZ）進行數據傳輸，並通過位填充機制解決同步問題。當連續出現 5 個相同位時，插入相反位以保持同步性和通信穩定性。

2. 主要內容

2.1 對後端伺服器的攻擊使其停止運行

本節我們決定實作 DNS 反射攻擊，旨在評估車輛後端伺服器在 UN R155 2.1 和 UN R155 13.1 條款下的合規性。DNS 反射攻擊涉及向開放的 DNS 解析器發送

偽造的 DNS 查詢，並將目標車輛的後端伺服器作為偽造的來源地址。解析器會將大量 DNS 響應發送給目標，耗盡其資源，導致拒絕服務。



圖二、DNS 反射攻擊示意圖

首先，攻擊者會指揮已被惡意軟體感染並受其控至的殭屍電腦群（Botnet），在指定的時間點同時發動攻擊。這些殭屍電腦會向未經妥善保護的 DNS 伺服器 (圖二中的 User's Primary DNS Server)發送大量偽造的 DNS 查詢封包，這些封包偽裝成來自受害者伺服器的 IP 地址，目的是觸發伺服器進行遞迴 DNS 查詢。 接著，未經妥善保護的 DNS 伺服器開始向根伺服器發出域名查詢請求。當根伺服器回覆該域名不存在時，它會提供其他可能擁有該資訊的伺服器位置。 根據根伺服器的指引，受害的 DNS 伺服器會繼續向另一個根伺服器發送查詢。該伺服器回傳可以解析該域名的 DNS 伺服器地址，通常是靠近查詢目標的伺服器。之後，未經妥善保護的 DNS 伺服器會向這個新伺服器發出最終的查詢，以獲取解析結果。 當最終的 DNS 伺服器回傳域名解析資料後，未經妥善保護的 DNS 伺服器會將結果回傳給發送查詢的來源 IP 地址，這個地址是由殭屍電腦偽造的受害者伺服器 IP。如此便達成攻擊的目的。 攻擊者會通過不斷重複這些步驟，最終導致受害者伺服器資源耗盡，無法提供正常的網絡服務，從而實現了對受害者伺服器的有效阻斷。

2.2 對更新伺服器或網路的拒絕服務攻擊

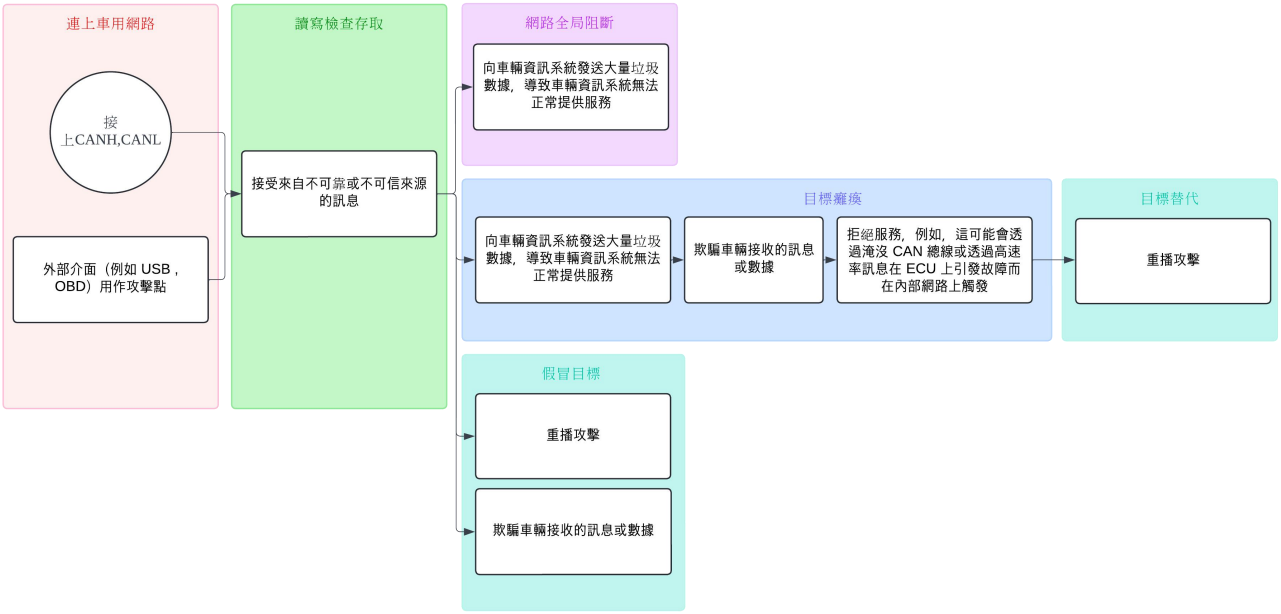
基本上手法與 2.1 對後端伺服器的攻擊使其停止運行一致，因為 DNS 反射攻擊的本質就是拒絕服務攻擊 (DOS)，利用過大的流量來阻斷伺服器的服務。

2.3 網路連接埠端口掃描

端口掃描是網絡安全中的一項關鍵技術，用於識別遠程主機上的開放端口和服務。通過了解哪些端口是開放的，網絡管理員可以更好地保護其系統，防止未經授權的訪問和漏洞。 我們編寫了一個使用 Python 的 socket 模塊的腳本。 如果端口是開放的，該腳本會記錄下來並嘗試識別該端口上運行的服務。它提供實時掃描進度更新，包括剩餘時間的估計。該腳本還包含錯誤處理功能，以處理無效的主機名或連接失敗等問題。掃描完成後，它會總結結果，顯示總耗時以及開放端口的狀態和對應服務的表格，為網絡安全評估提供有價值的信息。

2.4 車輛內部網路攻擊

針對車輛內部網路的攻擊，本遍將測試流程分爲以下幾個階段，如圖三，其中包含檢查車輛系統是否會接收不可靠或不可信來源的訊息、對車輛通訊系統發送欺騙訊息、重播攻擊、向車輛通訊系統發送大量垃圾數據，導致車輛資訊系統無法正常提供服務。

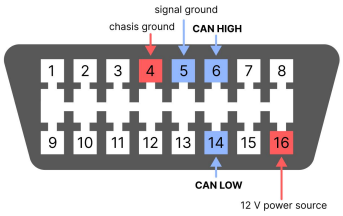


圖三、車輛內部網路攻擊流程圖

3. 實驗環境

3.1 連上車用網路

在這個步驟中，我們目的是連接上 CAN high 和 CAN low 進而能向 CAN 總線讀寫訊息。其中我們能直接對電路做外部連接或是透過外部介面，如 OBDII。



圖四、OBDII 示意圖

如圖四所示，OBD 將 pin 6 跟 pin 14 作為訪問 500kbps 的 CAN 網路，其所在的網路區段為較不重要的外部網路，依照各車廠設計，通常能存取方向盤的部分操作 多媒體操作、車燈操作、車窗控制、車鏡控制等。 接著進行 Baud Rate 搜尋，以確認網路頻率。常見的頻率有 33.333k、500k、250k、125k 和 1M。我們會針對每個頻率進行監聽，並計算 $T_{timeout}$ 時間內能解析的封包數量。若能在 $T_{timeout}$ 時間內能成功解析 N_{valid} 個封包，則該頻率被識別為網路的運行頻段。

3.2 讀寫檢查存取

一個有效的 CAN 幀 ACK 欄位是會被網路上的其他接收節點給覆寫的，因此我們透過檢查發送訊息的 ACK 欄來判斷當前注入點發送的訊息能否被其他節點接收。然而，讀取 CAN 幀內單個比特涉及韌體層的改動，本篇爲了能將測試泛化，利用 ACK 的錯誤處理機制。首先我們將發送一特定字段的封包，若此時有其他節點正在讀取此 ID 頻段的訊息，則會將 ACK 欄的隱性位元覆蓋，若否，則將引發 ACK 錯誤進而產生錯誤幀，因此我們能去檢測是否有錯誤幀的產生，依此來判斷輸入點是否有效。實作上我們會將攻擊控制器的重發功能關閉，以避免後續觸發錯誤循環。 若在發送後讀取到錯誤幀，則會再嘗試操作 $C_{threshold}$ 次，如此能避免其他錯誤，比如 CRC 錯誤，影響判斷結果。

3.3 網路全局阻斷

此部分的攻擊測試是對應到 UN R155 第 8.1 條款，向車輛通訊系統發送大量垃圾數據，導致車輛資訊系統無法正常提供服務。 由於 CAN 的仲裁機制，仲裁編號較小的訊息具有較高的優先級，因此我們在每次發送機會中佔據整個 CAN 通道。具體操作是透過不斷向 TX

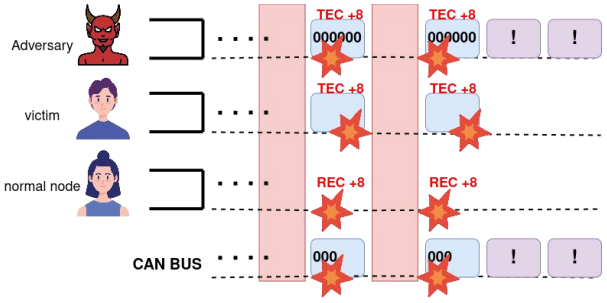
queue 塞入數據，向車輛信息系統發送大量垃圾數據。一般控制器的 TX FIFO queue 可容納 8 個 Frame，我們將從作業系統端使用開源工具包 can-utils 不斷填滿 TX queue，讓韌體自動在每個 IFS 結束後競爭 CAN Bus。實作上我們會尋找當前 CAN Bus 上仲裁 ID 的最低值 ID_m，並構建相應的 frame，具體格式為：id=0~IDm，length=0x8，內容為隨機數據。透過這種方式，攻擊者可以持續占據 CAN Bus 的競爭機會，最終導致車輛系統無法正常提供服務。

圖五、網路堵塞

如圖五所示，中間訊號及是 CAN 網路堵塞的實驗圖。

3.4 目標癱瘓

透過 CAN 對產生過多錯誤節點限制，我們故意誘導目標節點發生大量錯誤，最終導致其進入離線狀態。本研究提出了一種創新的方法，無需修改韌體，即可使目標節點癱瘓，這在泛化測試中具有明顯優勢。該方法可分為三個主要步驟：碰撞、錯誤循環，以及持續重新同步目標節點。 首先，攻擊 ECU 的請求需與目標 ECU 的輸出進行精確同步，目的是在 CAN 線路有傳輸機會時，使攻擊 ECU 與目標 ECU 能同時發送訊息並進入仲裁階段。我們通過網路全域阻斷，將目標的待傳輸訊息鎖定在其傳輸佇列中，當下一個仲裁階段結束後，便可以實現目標訊息與攻擊訊息的碰撞。 為了實現同步，我們會刻意測量目標封包的最長發送間隔時間 If，並在 CAN Bus 上進行與該間隔時間相等的阻斷操作，這樣能有效地創造出訊息碰撞的條件。 當攻擊 ECU 與目標 ECU 同步後，我們會發送與目標待發送訊息具有相同 ID 的訊息，使兩方同時獲得通道的發送權。在後續過程中，雙方在彼此不知情的情況下，同時向通道寫入訊息，訊息內容將相互影響。我們可以通過將攻擊訊息內容置換為顯性位來覆蓋目標的訊息，由於通道內容與預期寫入內容不符，目標 ECU 會發生錯誤。這種錯誤將觸發主動錯誤幀，引發通道的全局連鎖錯誤。在通道靜默 11 位元後，目標 ECU 因預設開啟自動重送功能，將會再次發送同一則訊息。如果我們同時將攻擊 ECU 也設置為自動重送，則雙方的重送訊息會再次發生碰撞，從而形成錯誤循環。如圖六

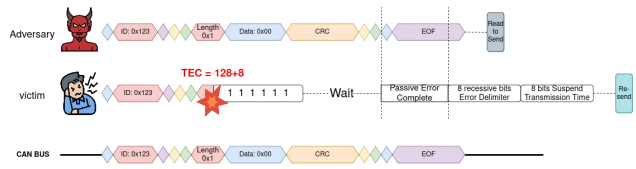


圖六、錯誤循環示意圖

錯誤循環會持續到目標 ECU 的傳送錯誤計數器超過 127，進而進入被動錯誤狀態。在此狀態下，目標 ECU 所產生的錯誤將不再影響整個通訊系統，這使得攻擊方能夠成功傳送訊息。同時，目標 ECU 必須等待被動錯誤幀的完成、錯誤分界符的結束以及被動錯誤懲罰的過程，才能再次嘗試重送訊息，如圖七。攻擊 ECU 和目標 ECU 因此失去同步。

為了使目標 ECU 的傳送錯誤計數器超過 255 並進入離線狀態，我們需要重新同步並製造更多錯誤。具體方法是在攻擊 ECU 傳送的攻擊訊息後，插入一個完整的冗餘訊息，而該訊息的內容部分包含一個 8 位元段。這樣，當目標 ECU 嘗試重送訊息時，該訊息將再次被卡在傳輸佇列中，無法順利發送。冗餘訊息結束後，攻擊 ECU 和目標 ECU 將重新同步，並再次同時競爭通道，這將導致更多的訊息碰撞與錯誤的發生。

因此，我們只需將攻擊 ECU 的攻擊訊息與冗餘訊息作為一組，並連續發送 16 組，便能使目標 ECU 的傳送錯誤計數器超過 255，最終進入離線狀態，達到目標癱瘓的目的。



圖七、時序同步示意圖

圖八、目標癱瘓圖

如圖八所示，在攻擊前受害者以穩定的頻率向 CAN 總線傳遞訊息，而受攻擊後(也就是指圖中間的部分)，受到攻擊訊息的惡意碰撞導致受害者進入 Bus off 狀態因而停止與總線連接的狀態。

3.5 目標替代

當目標節點癱瘓後，我們便可傳送先前錄製的目標監聽訊息，以假冒目標節點的身份進行通訊操作。透過這種方式，攻擊者可以模擬目標節點的行為，達成替代目標的效果。

3.6 假冒目標

CAN 通道以全局廣播方式傳送訊息，因此通過清空攻擊 ECU 的封包過濾表，我們可以監聽同一通道下的所有訊息，無需干擾正常通訊即可錄製目標的傳輸內容和識別 ID。一旦完成收集，我們便可利用錄製的訊息進行重播攻擊，或者根據收集到的識別 ID 偽造目標身份，並視需求填寫訊息內容，實現假冒目標節點的目的。

4 結論

本研究提出的 CAN 協議測試框架，顯著提升了汽車安全性檢驗的效率與精確性。該系統不僅能快速驗證車輛是否符合國際標準，如 UN R155，還能識別常見的資安漏洞，幫助車廠及測試機構有效提升車輛的安全性。通過標準化和流程的高度整合，我們大幅減少了測試所需的時間和資源，實現了檢驗成本的節約。 系統的分層式架構設計提供了極高的擴展性，能靈活應對各種攻擊手法，且具備全球應用性，適用於不同國家和市場的安全檢測需求。本工具的創新性在於其高度整合的測試框架，讓測試者能夠方便、全面地展開測試並快速獲得結果。與傳統方法相比，該系統顯著提升了攻擊流程的效率，並減少了對系統的影響，增強了測試的實用性和操作性。 總之，該研究成果不僅簡化了攻擊流程，還提升了系統的安全測試能力，為汽車工業提供了一個強大且高效的資安測試工具，具有長遠的應用價值。

5 致謝

感謝教授他們在實驗設計及技術實作方面提供了寶貴的貢獻。財團法人車輛測試研究中心的研究員們也提供了測試環境與技術支持，為本研究的順利進行提供了保障。這些研究不僅為我們的攻擊測試腳本設計有力的背景支持，也激發了我們在現有技術基礎上的創新與完善。感謝所有提供理論和技術參考的研究者們，他們的工作促成了本研究的完成。

6 參考文獻

[1] United Nations Economic Commission for Europe 2021, UN Regulation No. 155 - Cyber security and cyber security management system, accessed 18 September 2024
[2] S. Soderi, R. Colelli, F. Turrin, F. Pascucci and M. Conti, "SENECAN: Secure KEy DistributioN OvEr CAN Through Watermarking and Jamming," in IEEE Transactions on Dependable and Secure Computing, vol. 20, no. 3, pp. 2274-2288, 1 May-June 2023, doi: 10.1109/TDSC.2022.3179562.
[3] Zeinab El-Rewini, Karthikeyan Sadatsharan, Daisy Flora Selvaraj, Siby Jose Plathottam, Prakash Ranganathan,"Surity challenges in vehicular communications," Vehicular Communications,Volume 23,2020,100214,ISSN 2214-2096.
[4] Y. Zhao, G. Dan, A. Ruan, J. Huang and H. Xiong, "Q," 2021 IEEE Conference on Dependable and Secure Computing (DSC), Aizuwakamatsu, Fukushima, Japan, 2021, pp. 1-7, doi: 10.1109/DSC49826.2021.9346268.
[5] H. Zhang, Y. Pan, Z. Lu, J. Wang and Z. Liu, "A Cyber Security Evaluation Framework for In-Vehicle

Electrical Control Units," in IEEE Access, vol. 9, pp. 149690-149706, 2021, doi: 10.1109/ACCESS.2021.3124565.

[6] T. Balan, A. Balan and F. Sandu, "SDR Implementation of a D2D Security Cryptographic Mechanism," in IEEE Access, vol. 7, pp. 38847-38855, 2019, doi: 10.1109/ACCESS.2019.2904909.

[7] D. Yu, S. Lee, R. -H. Hsu and J. Lee, "Ensuring End-to-End Security With Fine-Grained Access Control for Connected and Autonomous Vehicles," in IEEE Transactions on Information Forensics and Security, vol. 19, pp. 6962-6977, 2024, doi: 10.1109/TIFS.2024.3417292.

[8] Taminul Islam, Md. Alif Sheakh, Anjuman Naher Jui, Omar Sharif, Md Zobaer Hasan,"A review of cyber attacks on sensors and perception systems in autonomous vehicle,"Journal of Economy and Technology,Volume 1,2023,Pages 242-258,ISSN 2949-9488,

[9] Jakobsen, S. B., Knudsen, K. S., & Andersen, B. (2023). "Analysis of Sensor Attacks against Autonomous Vehicles." In Proceedings of the 8th International Conference on Internet of Things, Big Data and Security - IoTBDS (Vol. 1, pp. 131-139). SCITEPRESS Digital Library

[10] Y. Li, Q. Luo, J. Liu, H. Guo and N. Kato, "TSP Security in Intelligent and Connected Vehicles: Challenges and Solutions," in IEEE Wireless Communications, vol. 26, no. 3, pp. 125-131, June 2019, doi: 10.1109/MWC.2019.1800289.

[11] Giannaros, A.; Karras, A.; Theodorakopoulos, L.; Karras, C.; Kranias, P.; Schizas, N.; Kalogeratos, G.; Tsolis, D. "Autonomous Vehicles: Sophisticated Attacks, Safety Issues, Challenges, Open Topics, Blockchain, and Future Directions" . J. Cybersecur. Priv. 2023, 3, 493-543.

[12] J. Liu, W. Sun, Yongpeng Shi, In-vehicle network attacks and countermeasures: challenges and future directions, IEEE Netw. 31 (2017) 50–58.

[13] W. Choi, K. Joo, H.J. Jo, M.C. Park, D.H. Lee, VoltageIDS: low-level communication characteristics for automotive intrusion detection system, IEEE Trans. Inf. Forensics Secur. 13 (2018) 2114–2129.

[14] P. Carsten, M. Yampolskiy, T.R. Andel, J.T. Mcdonald, In-vehicle networks: attacks, vulnerabilities, and proposed solutions, in: Proceedings of the 10th Annual Cyber and Information Security Research Conference, 2015.

[15] H. Ueda, R. Kurachi, H. Takada, T. Mizutani, M. Inoue, S. Horihata, Security authentication system for in-vehicle network, SEI Tech. Rev. (2015).

[16] N. Nowdehi, A. Lautenbach, T. Olovsson, In-vehicle CAN message authentication: an evaluation based on industrial criteria, in: IEEE 86th Vehicular Technology Conference, 2017.

[17] P. Mundhenk, S. Steinhorst, M. Lukasiewycz, S.A. Fahmy, S. Chakraborty, Lightweight authentication for secure automotive networks, in: Proceedings of the 2015 Design, Automation & Test in Europe Conference & Exhibition, 2015, pp. 285–288.

[18] K.D. Kang, Y. Baek, S. Lee, S.H. Son, An attack-resilient source authentication protocol in controller area network, in: ACM/IEEE Symposium on Architectures for Networking and Communications Systems, 2017, pp. 109–118.

[19] A. Tashiro, H. Muraoka, S. Araki, K. Kakizaki, S. Uehara, A secure protocol consisting of two different security-level message authentications over CAN, in: 3rd IEEE International Conference on Computer and Communications, 2017, pp. 1520–1524.

[20] W. Choi, H.J. Jo, S. Woo, J.Y. Chun, J. Park, D.H. Lee, Identifying ECUs using inimitable characteristics of signals in controller area networks, IEEE Trans. Veh. Technol. 67 (2018) 4757–4770.

[21] A. Tomlinson, J. Bryans, S.A. Shaikh, H.K. Kalutarage, Detection of automotive CAN cyber-attacks by identifying packet timing anomalies in time windows, in: 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops, 2018.

[22] H. Lee, S.H. Ergen, Jeong, H.K. Kim, OTIDS: a novel intrusion detection system for in-vehicle network by using remote frame, in: 15th Annual Conference on Privacy, Security and Trust (PST), 2017.

[23] B. Groza, P.S. Murvay, Security solutions for the controller area network: bringing authentication to in-vehicle networks, IEEE Veh. Technol. Mag. (2018) 40–47.

[24] Oleg Schell and Marcel Kneib. 2023. SPARTA: Signal Propagation-based Attack Recognition and Threat Avoidance for Automotive Networks. In Proceedings of the 2023 ACM Asia Conference on Computer and Communications Security (ASIA CCS '23). Association for Computing Machinery, New York, NY, USA, 760–772.