การประชุมวิชาการทางวิศวกรรมไฟฟ้า ครั้งที่ 48
The 48th Electrical Engineering Conference (EECON-48)
วันที่ 19-21 พฤศจิกายน 2568 ณ โรงแรมฟูราม่า จังหวัดเชียงใหม่

การตรวจจับการบุกรุกบนเครือข่ายแคนบัสในยานยนต์ด้วยเอ็กซ์ตรีมเลิร์นนิงแมชีน

Intrusion Detection on In-Vehicle CAN Bus Networks using Extreme Learning Machine

ชานนท์ ชูพงษ์* ณัฐพล หาอุปละ กันตินันท์ สกุลไพศาล ธีระพล เหมือนขาว และ มนฑล นาวงษ์

ภาควิชาวิศวกรรมไฟฟ้า คณะวิศวกรรมศาสตร์ มหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี charnon.c@en.rmutt.ac.th*

บทคัดย่อ

งานวิจัยนี้ได้นำเสนอการใช้โมเดลเอ็กซ์ตรีมเลิร์นนิงแมชีน เพื่อตรวจจับการบุกรุกบนเครือข่ายแคนบัสในยานยนต์ โดยใช้ค่าเอนโทรปีของข้อมูลในแคนบัสเป็นคุณลักษณะเด่นที่ใช้ตรวจจับ จากการทดลองพบว่าระบบที่นำเสนอนี้สามารถตรวจจับการบุกรุกในรูปแบบต่างๆ ได้อย่างแม่นยำ ผลการทดลองดังกล่าวได้นำไปเปรียบเทียบกับงานวิจัยอื่นที่ใกล้เคียงกัน ซึ่งใช้โมเดลวัน-คลาสซัพพอร์ตเวกเตอร์แมชีน ในการตรวจจับ ซึ่งพบว่าโมเดลดังกล่าวมีความผิดพลาด 3% ขณะที่โมเดลที่นำเสนอไม่มีข้อผิดพลาดในการตรวจจับการบุกรุก จากการศึกษานี้แสดงให้เห็นว่าเอ็กซ์ตรีมเลิร์นนิงแมชีน เป็นโมเดลที่มีศักยภาพสูงในการใช้งานตรวจจับการบุกรุกในแคนบัส

คำสำคัญ: ยานยนต์ แคนบัส การตรวจจับการบุกรุก

Abstract

This research presents the use of the Extreme Learning Machine model to detect intrusion on the automotive CAN bus network by using the entropy of CAN bus data as a feature for detection. The experiments show that the proposed system can detect various types of intrusions accurately. The experimental results are compared with other similar research that uses the One-Class Support Vector Machine model for detection. It is found that the model has an error of 3%, while the proposed model has no error in detecting intrusion. This study shows that extreme machine learning is a model with high potential for detecting intrusions in CAN bus.

Keywords: Automotive, CAN bus, Intrusion detection

1. บทนำ

ในปัจจุบัน ระบบรถยนต์สมัยใหม่มีการนำเทคโนโลยีอิเล็กทรอนิกส์และระบบควบคุมต่าง ๆ มาทำงานร่วมกันอย่างซับซ้อนผ่านเครือข่ายสื่อสารภายในรถ โดยระบบ Controller Area Network (CAN Bus) เป็นโปรโตคอลหลักที่ใช้ในการแลกเปลี่ยนข้อมูลระหว่างหน่วยควบคุมอิเล็กทรอนิกส์ (Electronic Control Unit: ECU) ต่าง ๆ เช่น ระบบเบรก ระบบเครื่องยนต์ ระบบถุงลมนิรภัย และระบบช่วยขับขี่อัตโนมัติ จุดเด่นของ CAN Bus คือมีโครงสร้างที่เรียบง่าย ประสิทธิภาพสูง และต้นทุนต่ำ จึงได้รับความนิยมอย่างแพร่หลายในอุตสาหกรรมยานยนต์ อย่างไรก็ตาม ความเรียบง่ายของ CAN Bus ส่งผลให้ไม่มีการออกแบบกลไกด้านความปลอดภัยมาโดยตรง [1] เช่น การยืนยันตัวตน การเข้ารหัส หรือการควบคุมการเข้าถึง ทำให้ผู้ไม่หวังดีสามารถบุกรุกหรือปลอมแปลงข้อมูลบนเครือข่าย CAN ได้ค่อนข้างง่าย ส่งผลกระทบต่อความปลอดภัยของระบบรถยนต์โดยรวม ในช่วงหลายปีที่ผ่านมา ได้มีรายงานการโจมตีที่ตอกย้ำถึงความสำคัญของการตรวจจับการบุกรุกบนเครือข่าย CAN Bus เช่น กรณีที่นักวิจัยด้านความปลอดภัยสามารถเข้าควบคุมระบบเบรกและพวงมาลัยของรถยนต์ได้จากระยะไกลผ่านช่องโหว่ของระบบสื่อสารภายใน [2] หรือกรณีการโจมตีโดยการส่งข้อความปลอมเพื่อปิดการทำงานของระบบถุงลมนิรภัย [3] เหตุการณ์เหล่านี้สะท้อนให้เห็นว่าการพัฒนาระบบตรวจจับการบุกรุกสำหรับรถยนต์เป็นสิ่งจำเป็นอย่างยิ่ง เพื่อป้องกันอุบัติเหตุและรักษาความปลอดภัยของผู้โดยสาร

ซึ่งที่ผ่านมาได้มีการนำเสนอระบบตรวจจับการบุกรุกในแคนบัสจำนวนหนึ่งตัวอย่างเช่น ใน [4] ซึ่งใช้โครงข่ายประสาทเทียมเชิงลึก (Deep Neural Network) หรือใน [5] ซึ่งใช้โมเดลหน่วยความจำระยะสั้นแบบยาว (Long Short-Term Memory, LSTM) ในการแยกแยะข้อความใน CAN bus ว่าเป็นข้อความที่ส่งมาจากผู้บุกรุกหรือไม่ โดยโมเดลเหล่านี้จำเป็นต้องใช้ข้อมูลฝึกสอนจำนวนมากและการคำนวณที่ซับซ้อน แต่ ECU ส่วนใหญ่ในรถยนต์มีข้อจำกัดด้านกำลังประมวลผลและหน่วยความจำ การเลือกใช้เทคนิคที่ไม่ซับซ้อน จึงเป็นทางเลือกที่เหมาะสมอย่างยิ่งสำหรับการประยุกต์ใช้ในบริบทของยานยนต์จริง [6]

ดังนั้นในบทความนี้จึงนำเสนอระบบการตรวจจับการบุกรุกใน CAN Bus ด้วย Extreme Learning Machine (ELM) ซึ่งเป็นโมเดลการเรียนรู้ของเครื่อง (Machine Learning Model) ที่มีความซับซ้อนต่ำ ทำงานได้รวดเร็วและแม่นยำ

2. ทฤษฎีที่เกี่ยวข้อง

2.1 รูปแบบข้อความใน CAN Bus

ข้อความในการสื่อสารด้วย CAN Bus จะเป็นไปตามมาตรฐาน ISO 11898 หรือมักจะเรียกกันว่า CAN 2.0 [7] โดยในข้อความจะต้องประกอบด้วยส่วนต่างๆ ที่เรียกรวมกันว่าเฟรมของข้อความ ดังรูปที่ 1 ซึ่งในเฟรมดังกล่าวจะมีส่วนที่สำคัญอยู่ 2 ส่วนที่มักถูกนำไปใช้ในการวิเคราะห์คือ CAN ID และ Data โดย ID จะเป็นหมายเลขประจำตัวของเฟรมข้อมูลหนึ่งๆ เช่น เฟรมที่ส่งข้อมูลความเร็วของรถยนต์ หรือเฟรมที่ส่ง

*ผู้ประพันธ์บรรณกิจ

ข้อมูลแรงดันไฟฟ้าของแบตเตอรี่ ก็จะมี CAN ID ที่แตกต่างกัน และส่วน Data เป็นส่วนของข้อมูลจริงที่ ECU ต้องการส่งเข้ามาใน CAN Bus

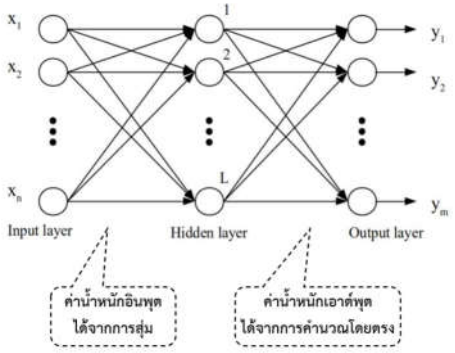
Start 1 bit	CAN ID 11 or 29 bits	RTR 1 bit	Reserved 2 bits	Data Length 4 bits	Data 0-64 bits	CRC 16 bits	ACK 2 bits	EOF 7 bits

รูปที่ 1 ส่วนประกอบของข้อความใน CAN Bus

ในบทความนี้ได้ใช้ค่า CAN ID เป็นตัวตรวจจับการบุกรุกใน CAN Bus โดยนำ CAN ID มาผ่านการสกัดคุณลักษณะเด่นบางอย่างและป้อนเข้าโมเดล ELM เพื่อทำการจำแนกว่าเป็นข้อความจากการบุกรุกหรือไม่ ซึ่งรายละเอียดจะกล่าวในหัวข้อถัดไป

2.2 Extreme Learning Machine (ELM)

ELM เป็นโมเดลโครงข่ายประสาทเทียมแบบฟีดฟอร์เวิร์ดที่มีชั้นซ่อนชั้นเดียวที่ถูกนำเสนอโดย Guang-Bin Huang [8] ซึ่งมีการฝึกสอน (Training) ที่แตกต่างไปจากโมเดลโครงข่ายประสาทเทียมทั่วไปคือค่าน้ำหนักในชั้นซ่อนจะได้มาจากการสุ่มค่า ส่วนค่าน้ำหนักในชั้นเอาต์พุตได้มาจากการคำนวณค่าทางพีชคณิตโดยตรง ซึ่งช่วยให้โมเดลสามารถเรียนรู้จากข้อมูลได้เร็วกว่าโครงข่ายประสาทเทียมปกติหลายเท่าตัวโดยที่ยังคงมีความแม่นยำไม่แตกต่างจากเดิม [9] โครงสร้างของ ELM เป็นดังรูปที่ 2



รูปที่ 2 โครงสร้างของโมเดล ELM

กำหนดให้ (x_j, y_j) เป็นอินพุตและเอาต์พุตตัวอย่างที่ใช้สอนโมเดลซึ่งมีจำนวน k ชุด โดย $x_j \in \mathbb{R}^n$ และ $y_j \in \mathbb{R}^m$ โมเดลมีจำนวนโหนดในชั้นซ่อนเท่ากับ L ความสัมพันธ์ระหว่างค่าอินพุตและเอาต์พุตจะเป็นไปตามสมการที่ 1 ดังนี้ [4]

$$y_j = \sum_{i=1}^{L} \beta_i G(a_i x_j + b_i), \quad j = 1,2,3,...K \tag{1}$$

โดย $a_i \in \mathbb{R}^n$ และ $b_i \in \mathbb{R}$ คือค่าน้ำหนักและค่าไบอัสในชั้นอินพุต ซึ่งได้จากการสุ่มและค่านี้จะคงที่ตลอดการใช้งานโมเดล, $G(..)$ เป็นฟังก์ชันของโหนดในชั้นซ่อนซึ่งเหมือนกับโครงข่ายประสาทเทียมทั่วไป และ $\beta_i \in \mathbb{R}^m$ คือค่าน้ำหนักในชั้นเอาต์พุต สมการที่ (1) สามารถเขียนใหม่อย่างง่ายได้ดังนี้

$$\mathbf{Y} = \mathbf{H}\boldsymbol{\beta} \tag{2}$$

โดย

$$\mathbf{H} = \begin{bmatrix} G(a_1 x_1 + b_1) & \cdots & G(a_L x_1 + b_L) \\ \vdots & \ddots & \vdots \\ G(a_1 x_K + b_1) & \cdots & G(a_L x_K + b_1) \end{bmatrix}_{K \times L}$$

$$\mathbf{Y} = \begin{bmatrix} \mathbf{y}_1 \\ \vdots \\ \mathbf{y}_K \end{bmatrix}_{K \times m}, \quad \text{and} \quad \boldsymbol{\beta} = \begin{bmatrix} \boldsymbol{\beta}_1 \\ \vdots \\ \boldsymbol{\beta}_L \end{bmatrix}_{L \times m}$$

การสอนโมเดล (Training) คือการคำนวณหาค่า $\boldsymbol{\beta}$ โดยที่ทราบค่า $\mathbf{H}$ และค่า $\mathbf{Y}$ โดยใช้สมการต่อไปนี้

$$\boldsymbol{\beta} = \mathbf{H}^{\dagger}\mathbf{Y} \tag{3}$$

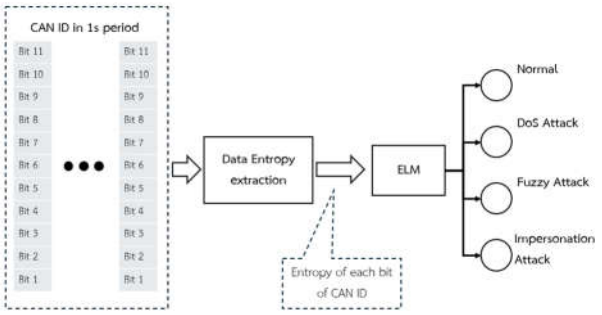
โดย $\mathbf{H}^{\dagger}$ คือการทำเมทริกซ์คล้ายผกผัน (Pseudo Inverse Matrix) ซึ่งสามารถคำนวณได้ดังนี้

$$\mathbf{H}^{\dagger} = (\mathbf{H}^{\mathrm{T}}\mathbf{H} + \lambda\mathbf{I})^{-1}\mathbf{H}^{\mathrm{T}} \tag{4}$$

ค่า $\lambda\mathbf{I}$ ในสมการที่ 4 เป็นค่า Regularization Factor ซึ่งมีค่าน้อยมากบวกเพิ่มให้กับสมาชิกในเส้นทแยงมุมของเมทริกซ์เพื่อป้องกันปัญหาจากเมทริกซ์ที่ไม่สามารถแปลงผกผันได้ (Non-inverting Matrix) [10]

3. ระบบที่นำเสนอ

ระบบตรวจจับการบุกรุกในแคนบัสที่นำเสนอในบทความนี้ใช้การบันทึกค่า CAN ID ของทุกข้อความในช่วง 1 วินาทีมาทำการสกัดคุณลักษณะเด่น ของข้อมูลซึ่งในที่นี้เลือกใช้ค่าเอนโทรปี (Entropy) ของข้อมูล CAN ID ในแต่ละบิต จากนั้นนำค่า Entropy ของทั้ง 11 บิตที่ได้นำเข้าโมเดล ELM เพื่อทำการจำแนกประเภท (Classification) ของข้อความในช่วง 1 วินาทีดังกล่าวว่าเป็นข้อความประเภทใด โดยโมเดล ELM นี้ได้รับการฝึกสอนให้สามารถจำแนกประเภทข้อความได้ 4 ประเภท ภาพรวมของระบบที่นำเสนอแสดงได้ดังรูปที่ 3 โดยรายละเอียดของแต่ละส่วนสามารถอธิบายได้ดังนี้



รูปที่ 3 แผนผังของระบบที่นำเสนอ

ส่วน Data Entropy Extraction รับข้อมูล CAN ID ของทุกข้อความใน CAN Bus ในช่วงเวลา 1 วินาทีซึ่งแต่ละข้อความจะมี CAN ID ขนาด 11 บิต และนำมาคำนวณค่า Entropy ของแต่ละบิตดังสมการที่ (5) [11] ซึ่งค่า Entropy ของ CAN ID ทั้ง 11 บิตในช่วงเวลา 1 วินาทีนี้สามารถบอกถึงรูปแบบของ CAN ID ของข้อความที่สื่อสารกันใน CAN Bus ได้

$$H(x) = -\sum_{i=0,1} p(x_i)\log_2 p(x_i) \qquad (5)$$

โดย

$H(x)$ หมายถึงค่า Entropy ของ CAN ID แต่ละบิต

$p(x_i)$ เมื่อ i =0 หมายถึง ความน่าจะเป็นที่บิตนี้จะมีค่าเป็นลอจิก 0

$p(x_i)$ เมื่อ i =1 หมายถึง ความน่าจะเป็นที่บิตนี้จะมีค่าเป็นลอจิก 1

โมเดล ELM ที่ใช้ในบทความนี้มีขนาด 11 อินพุตตามจำนวนขนาดของข้อมูล Entropy ของ CAN ID ที่เป็นข้อมูลอินพุต ในชั้นซ่อนมีขนาด 80 โหนดและใช้ Sigmoid เป็นฟังก์ชันกระตุ้น (Activation function) ในส่วนเอาต์พุตมีขนาด 4 โหนด ซึ่งสามารถจำแนกประเภทของข้อความได้ 4 ประเภท รายละเอียดของข้อความแต่ละประเภทมีดังนี้ 1) ปกติ (Normal) เป็นสภาวะที่ CAN Bus ทำงานแบบปกติไม่มีผู้บุกรุก 2) Denial of Service (DoS) Attack เป็นสภาวะที่มีผู้บุกรุกส่งข้อความที่มีลำดับความสำคัญสูง (High priority message) เพื่อรบกวนการสื่อสาร ส่งผลให้ ECU ตัวอื่นไม่สามารถใช้งาน Bus ได้ 3) Fuzzy Attack เป็นสภาวะที่ผู้บุกรุกส่งข้อความแบบสุ่มไปใน CAN Bus โดยหวังให้เกิดข้อผิดพลาดในการทำงานของ ECU และ 4) Impersonation (IM) Attack เป็นสภาวะที่ผู้บุกรุกส่งข้อความเข้าไปใน CAN bus โดย “ปลอมตัว” ให้เสมือนเป็น ECU จริงในระบบ

4. การทดลองและผลการทดลอง

การทดลองในบทความนี้ได้ใช้ชุดข้อมูล (Dataset) ที่ชื่อว่า CAN Dataset for Intrusion Detection [12] ซึ่งเป็นข้อความใน CAN Bus ที่แยกประเภทไว้เป็น 4 ประเภท (4 Class) ตามที่ได้กล่าวถึงในหัวข้อที่แล้ว จากนั้นจัดกลุ่มข้อมูลตามค่า Time Stamp โดยแบ่งข้อมูลเป็นช่วง ช่วงละ 1 วินาที แล้วจึงคำนวณค่า Entropy ในแต่ละบิตของ CAN ID ตามสมการที่ (5) จะได้ค่าอินพุตที่ใช้ในการฝึกสอนและทดสอบ ซึ่งแต่ละตัวอย่างเป็นเวกเตอร์ 1 มิติที่มีสมาชิก 11 ตัว และใช้ค่า ประเภทของข้อมูลเข้ารหัสแบบ One-hot Encoding เป็นค่าเป้าหมาย (Target)

ในการฝึกสอนโมเดล ELM ใช้ข้อมูลตัวอย่างจาก Dataset ที่ทำการคำนวณค่า Entropy ในแต่ละบิตของ CAN ID แล้วจำนวน 200 ตัวอย่างต่อประเภทของข้อมูลรวมเป็นข้อมูลตัวอย่างทั้งสิ้น 800 ตัวอย่าง ทำการฝึกสอนแบบตรวจสอบไขว้ที่แบ่งข้อมูลเป็น 8 พับ (8 fold cross validation) ฝึกสอนด้วยตัวอย่าง 700 ตัวและตรวจสอบด้วยตัวอย่าง 100 ตัวอย่างไขว้กันไป ทำให้ได้จำนวนโหนดในชั้นซ่อนที่เหมาะสมคือ 80 โหนด ส่วนการทดสอบการทำงานของระบบ ใช้ข้อมูลตัวอย่างจาก Dataset ที่ทำการคำนวณค่า Entropy ในแต่ละบิตของ CAN ID แล้วจำนวน 100 ตัวอย่างต่อประเภทของข้อมูล ซึ่งรวมเป็นข้อมูลตัวอย่างทั้งสิ้น 400 ตัวอย่างที่ไม่ได้นำไปฝึกสอนโมเดล ผลการทดสอบแยกแยะประเภทข้อความ CAN Bus แสดงใน Confusion Matrix ดังตารางที่ 1

ตารางที่ 1 ผลการทดลองของระบบที่นำเสนอ

จำนวนตัวอย่างแต่ละประเภทของข้อมูล		ประเภทที่ทำนาย			
		Normal	DoS Attack	Fuzzy Attack	IM Attack
ประเภทจริง	Normal	100	0	0	0
	DoS Attack	0	100	0	0
	Fuzzy Attack	0	0	100	0
	IM Attack	0	0	0	100

เพื่อเปรียบเทียบระบบที่นำเสนอกับระบบอื่นที่ใกล้เคียงกัน บทความนี้จึงได้นำผลจากระบบตรวจจับการบุกรุกใน CAN Bus อีกบทความหนึ่ง [13] ซึ่งใช้ Entropy ของ CAN ID เป็น Feature ของข้อมูลอินพุตเหมือนกับที่นำเสนอในบทความนี้ แต่โมเดลที่ใช้จำแนกประเภทของข้อความ CAN bus ในบทความดังกล่าวได้เลือกใช้ One-Class Support Vector Machine (OCSVM) ซึ่งเป็นโมเดลที่สามารถแยกแยะข้อความได้ 2 ประเภทคือข้อความปกติกับข้อความที่ผิดปกติ การทดลองของบทความดังกล่าวใช้ dataset เดียวกันกับที่นำเสนอในบทความนี้ ผลการทดลองของบทความดังกล่าวเป็นดังตารางที่ 2

ตารางที่ 2 ผลการทดลองของระบบที่นำมาเปรียบเทียบ

จำนวนตัวอย่างแต่ละประเภท		ประเภทที่ทำนาย	
		Normal	Anomaly
ประเภทจริง	Normal	97	3
	Anomaly	0	100

5. วิเคราะห์ผลการทดลอง

จากตารางที่ 1 ผลการทดลองของระบบที่นำเสนอ และตารางที่ 2 ผลการทดลองของระบบที่นำมาเปรียบเทียบ พบว่าระบบที่นำเสนอสามารถจำแนกประเภท (Classify) ของข้อความใน CAN Bus ได้อย่างถูกต้อง 100% ในทุกประเภทของข้อความ ส่วนระบบที่ใช้เปรียบเทียบมีความผิดพลาดในการจำแนกข้อความปกติอยู่ 3% ส่วนข้อความที่ผิดปกติสามารถจำแนกได้อย่างถูกต้อง 100% สาเหตุที่โมเดล ELM ที่นำเสนอมีความแม่นยำสูงกว่าเนื่องจากได้รับการฝึกสอนด้วยข้อมูลทุกประเภททำให้โมเดลสร้างเงื่อนไขการจำแนกได้อย่างถูกต้อง โดยเฉพาะเมื่อใช้ Feature ที่แยกแยะข้อมูลได้อย่างชัดเจนเช่น Data Entropy ส่วนโมเดล OCSVM นั้นได้รับการฝึกสอนด้วยข้อมูลประเภทปกติ (Normal class) เท่านั้น ทำให้โมเดลสร้างเงื่อนไขการจำแนกได้ไม่สมบูรณ์

6. สรุป

จากการทดลองพบว่าโมเดล ELM ให้ความแม่นยำสูงถึง 100% ในทุกประเภทข้อความ ส่วนโมเดล OCSVM ที่เป็นโมเดลแบบ One-class Classification มีความแม่นยำต่ำกว่าเล็กน้อยโดยเกิดข้อผิดพลาด 3% ในการจำแนกข้อความประเภทปกติ อย่างไรก็ตามโมเดล OCSVM มีข้อได้เปรียบในการใช้งานคือ ไม่จำเป็นต้องมีข้อมูลตัวอย่างของข้อความที่มีการบุกรุก เหมาะกับกรณีที่ไม่สามารถหาข้อมูลตัวอย่างได้ครบถ้วน ส่วนโมเดล ELM ที่มีความแม่นยำสูงจำเป็นจะต้องมีข้อมูลตัวอย่างที่ครบถ้วนสำหรับการพัฒนาต่อยอดผู้เขียนจะทำการพัฒนาโมเดลที่มีจุดเด่นของทั้ง2 โมเดล คือให้ความแม่นยำสูง สามารถแยกแยะประเภทของข้อความบุกรุกและไม่เป็นต้องใช้ข้อมูลฝึกสอนจำนวนมากนัก

เอกสารอ้างอิง

[1] C. Young, J. Zambreno, H. Olufowobi and G. Bloom, "Survey of Automotive Controller Area Network Intrusion Detection Systems," in IEEE Design & Test, vol. 36, no. 6, pp. 48-55, Dec. 2019.

[2] C. Valasek and C. Miller, “Remote Exploitation of an Unaltered Passenger Vehicle,” IOActive, 2015. [Online]. Available: https://www.ioactive.com/wp-content/uploads/pdfs/IOActive_Remote_Car_Hacking.pdf

[3] K. Koscher et al., “Experimental Security Analysis of a Modern Automobile,” in Proc. IEEE Symp. Security and Privacy, Oakland, CA, USA, May 2010, pp. 447–462.

[4] M.-J. Kang and J.-W. Kang, “A novel intrusion detection method using deep neural network for in-vehicle network security,” in Proc. IEEE 83rd Veh. Technol. Conf. (VTC Spring), Nanjing, China, May 2016, pp. 1–5.

[5] A. Taylor, S. Leblanc, and N. Japkowicz, “Anomaly detection in automobile control network data with long short-term memory networks,” in Proc. IEEE Int. Conf. Data Sci. Advanced Anal. (DSAA), Montreal, QC, Canada, Oct. 2016, pp. 130–139.

[6] J. Khan, D.-W. Lim, and Y.-S. Kim, "Intrusion detection system CAN-bus in-vehicle networks based on the statistical characteristics of attacks," Sensors, vol. 23, no. 7, p. 3554, 2023.

[7] ISO, “ISO 11898-1:2015 – Road vehicles — Controller area network (CAN) — Part 1: Data link layer and physical signalling,” International Organization for Standardization, Geneva, Switzerland, 2015.

[8] Guang-Bin Huang, Qin-Yu Zhu and Chee-Kheong Siew, "Extreme learning machine: a new learning scheme of feedforward neural networks," 2004 IEEE International Joint Conference on Neural Networks (IEEE Cat. No.04CH37541), Budapest, Hungary, 2004, pp. 985-990.

[9] Wang, J., Lu, S., Wang, SH. et al. A review on extreme learning machine. Multimed Tools Appl 81, 41611–41660, 2022.

[10] [1] G.-B. Huang, Q.-Y. Zhu, and C.-K. Siew, "Extreme learning machine: Theory and applications," Neurocomputing, vol. 70, no. 1–3, pp. 489–501, 2006.

[11] Q. Wang, Z. Lu and G. Qu, "An Entropy Analysis Based Intrusion Detection System for Controller Area Network in Vehicles," 2018 31st IEEE International System-on-Chip Conference (SOCC), Arlington, VA, USA, 2018.

[12] H. Lee, S. H. Jeong and H. K. Kim, "OTIDS: A Novel Intrusion Detection System for In-vehicle Network by Using Remote Frame," 2017 15th Annual Conference on Privacy, Security and Trust (PST), Calgary, AB, Canada, 2017, pp. 57-5709.

[13] C. Chupong, N. Junhuathon, K. Kitwattana, T. Muankhaw, N. Ha-Upala and M. Nawong, "Intrusion Detection in CAN Bus using the Entropy of Data and One-class Classification," 2024 International Conference on Power, Energy and Innovations (ICPEI), Nakhon Ratchasima, Thailand, 2024, pp. 157-160.