Electron: Jurnal Ilmiah Teknik Elektro
p-ISSN 2830–523X | e-ISSN 2622–6588
Volume 6 Nomor 1 Mei 2025

Tinjauan Literatur: Deteksi Anomali Berbasis Analisis Waktu pada CAN Bus Kendaraan Listrik

Literature Review: Timing Analysis Based Anomaly Detection on Electric Vehicle CAN Bus

Putu Ayu Citra Setiawan[1], Ida Ayu Dwi Giriantari[2], Ngurah Indra ER[3]

[1] Program Studi Magister Teknik Elektro Universitas Udayana, Gedung Pacasarjana Universitas Udayana; email: setiawan.2381711026@student.unud.ac.id
[2,3] Jurusan Teknik Elektro Fakultas Teknik Universitas Udayana; email: 2 dayu.giriantari@unud.ac.id, 3indra@unud.ac.id

[Dikirimkan: 7 Januari 2025, Direvisi: 23 Mei 2025, Diterima: 31 Mei 2025]
Corresponding Author: Putu Ayu Citra Setiawan

INTISARI — Perkembangan teknologi otomotif modern menekankan pentingnya konektivitas dan otonomi kendaraan, dengan tujuan meningkatkan keselamatan dan kenyamanan. Salah satu aspek krusial dari kendaraan modern adalah sistem komunikasi antar ECU (Electronic Control Units), yang sebagian besar menggunakan CAN Bus sebagai protokol utama. CAN Bus mengatur berbagai fungsi vital kendaraan, mulai dari sistem pengereman hingga fitur keselamatan, yang menjadikannya target potensial bagi ancaman keamanan. Oleh karena itu, industri otomotif mengembangkan dua pendekatan utama untuk mengatasi masalah keamanan ini. Pertama, pertahanan pasif melalui protokol keamanan yang mencakup enkripsi, otentikasi, dan verifikasi pesan dan kedua, deteksi anomali yang menggunakan teknologi canggih. Beberapa metode deteksi anomali yang telah diperkenalkan antara lain K-Means clustering, Support Vector Machines (SVM), dan Deep Learning, masing-masing menawarkan keunggulan dalam mendeteksi pola serangan tertentu. Namun, salah satu pendekatan yang semakin populer adalah analisis waktu, yang memanfaatkan pola waktu antar pesan dan clock skew pada CAN Bus untuk mengidentifikasi perilaku mencurigakan dan mendeteksi anomali secara real-time. Meskipun metode ini telah menunjukkan efektivitas dalam mendeteksi berbagai jenis serangan, tantangan utama adalah kemampuannya dalam mengidentifikasi serangan yang sangat tersembunyi dan tidak terlihat oleh metode tradisional. Penelitian ini memberikan pemahaman tentang berbagai pendekatan deteksi anomali pada jaringan CAN Bus kendaraan listrik, dengan fokus utama pada analisis waktu. Dengan mengkaji berbagai pendekatan, penelitian ini memberikan wawasan yang berharga dalam meningkatkan keamanan kendaraan listrik dan ekosistem transportasi cerdas secara keseluruhan. Hasil penelitian menunjukkan bahwa metode berbasis analisis waktu dapat mendeteksi berbagai jenis serangan, seperti spoofing, replay attacks, dan denial-of-service (DoS), dengan efisiensi tinggi.

KATA KUNCI — Analisis Waktu Kedatangan, Deteksi Anomali, Jaringan Area Kontroler, Kendaraan Listrik, Offset Jam, Skew Jam.

ABSTRACT — The development of modern automotive technology emphasizes the importance of vehicle connectivity and autonomy, with the aim of enhancing safety and comfort. Due to its role in managing critical vehicle functions and its vulnerability to security threats, the automotive industry has developed two primary approaches to address CAN Bus security. Therefore, the automotive industry has developed two main approaches to address this security issue. First, passive defense through security protocols that include encryption, authentication, and message verification, and second, anomaly detection using advanced technologies. Several anomaly detection methods have been introduced, including K-Means clustering, Support Vector Machines, and Deep Learning, each offering advantages in detecting specific attack patterns. However, one increasingly popular approach is time analysis, which leverages message inter-arrival patterns and clock skew on the CAN Bus to identify suspicious behavior and detect anomalies in real-time. Although this method has shown effectiveness in detecting various types of attacks, the main challenge lies in its ability to identify highly concealed attacks that may not be visible to traditional methods. This research provides an understanding of various anomaly detection approaches on electric vehicle CAN Bus networks, with a primary focus on time analysis. By reviewing several approaches, this study offers valuable insights into improving the security of electric vehicles and the overall smart transportation ecosystem. The results show that time-based analysis methods can detect various types of attacks, such as spoofing, replay attacks, and denial-of-service, with high efficiency.

KEYWORDS — Anomaly Detection, Clock Offsets, Clock Skew, Controller Area Network, Kendaraan Listrik, Time Arrival Analysis.

I. PENDAHULUAN

Perkembangan industri otomotif saat ini bergerak pesat ke arah di mana konektivitas dan otonomi menjadi fitur utama dalam desain dan pengoperasian kendaraan. Inovasi dalam teknologi kendaraan, seperti kendaraan yang terhubung dan kendaraan dengan kemampuan mengemudi otonom (autonomous vehicles), diharapkan akan merombak paradigma transportasi masa depan. Kendaraan yang terhubung memungkinkan komunikasi antar kendaraan (Vehicle to Vehicle) dan antara kendaraan dengan

infrastruktur jalan, yang dapat meningkatkan kesadaran situasional dan mendukung pengambilan keputusan secara real-time untuk mengurangi potensi kecelakaan. Kendaraan otonom dikembangkan dengan tujuan mengurangi jumlah kecelakaan lalu lintas yang disebabkan oleh faktor manusia [3], seperti kelelahan atau kesalahan pengemudi. Dengan sistem kontrol yang sepenuhnya otomatis, kendaraan ini dapat menghindari kecelakaan dengan memanfaatkan sensor canggih, kamera, radar, dan algoritma kecerdasan buatan (AI) untuk mengidentifikasi dan merespons potensi bahaya lebih cepat daripada manusia. Selain itu, kendaraan otonom juga berpotensi mengurangi kemacetan lalu lintas, karena mereka dapat mengoptimalkan alur lalu lintas dengan berkoordinasi secara langsung dengan kendaraan lain, mengatur kecepatan dan jalur secara efisien, serta meminimalkan jeda antara kendaraan. Meskipun potensi manfaatnya besar, pengembangan kendaraan yang terhubung dan otonom juga menghadirkan tantangan baru, terutama dalam hal keamanan dan privasi [1][2][3]. Kendaraan yang terhubung memerlukan sistem komunikasi yang aman untuk mencegah potensi serangan siber, sementara kendaraan otonom perlu dipastikan dapat beroperasi dengan aman dalam lingkungan yang kompleks dan dinamis. Oleh karena itu, industri otomotif harus terus mengembangkan dan mengimplementasikan solusi teknologi yang tidak hanya memperhatikan inovasi dan kenyamanan, tetapi juga mengutamakan aspek keamanan dan perlindungan data pribadi pengguna.

CAN Bus (Controller Area Network) adalah protokol komunikasi yang digunakan dalam kendaraan modern, termasuk kendaraan listrik. Keamanan jaringan CAN bus menjadi masalah yang krusial karena potensi serangan yang dapat merusak sistem kendaraan dan membahayakan keselamatan karena Bus CAN berfungsi sebagai saluran komunikasi utama antar ECU yang mengatur berbagai fitur kendaraan, seperti sistem pengereman, pengendalian mesin, suspensi, sistem hiburan, dan bahkan fitur keselamatan seperti airbag. Karena itu serangan yang dilakukan terhadap bus CAN dan ECU memiliki potensi untuk mengakses dan mengendalikan berbagai subsistem kendaraan [3]. Jika ada serangan yang berhasil menembus sistem ini, pelaku dapat mengontrol atau mengubah fungsi-fungsi vital kendaraan.

Untuk meningkatkan keamanan jaringan kendaraan, terdapat dua pendekatan utama yang dapat diambil. Pendekatan pertama adalah melalui pertahanan pasif, yang berfokus pada pengembangan dan penerapan protokol keamanan atau kerangka jaringan keamanan untuk melindungi komunikasi di dalam kendaraan dan antara kendaraan dengan sistem luar. Protokol keamanan ini biasanya mencakup enkripsi, otentikasi, kontrol akses, dan verifikasi pesan untuk mencegah potensi serangan yang bisa mengeksploitasi celah keamanan di dalam sistem kendaraan. Beberapa protokol ini dapat menangkal serangan seperti man-in-the-middle, spoofing, dan replay attacks, yang dapat merusak integritas data yang dikirimkan di dalam jaringan kendaraan. Namun, meskipun protokol keamanan pasif ini dapat memberikan lapisan perlindungan, mereka tidak dapat sepenuhnya mengatasi ancaman yang terus berkembang, terutama serangan yang terjadi setelah akses ke jaringan kendaraan diperoleh. Oleh karena itu, pendekatan kedua yang semakin mendapatkan perhatian adalah melalui deteksi anomali berbasis teknologi canggih [4].

Deteksi anomali berfokus pada pemantauan dan analisis aktivitas jaringan kendaraan untuk mengidentifikasi pola yang tidak biasa atau mencurigakan yang mungkin menunjukkan adanya serangan atau pelanggaran keamanan. Tujuan utama dari deteksi anomali ini adalah untuk mendeteksi aktivitas yang menyimpang dari pola komunikasi normal, yang sering kali mengindikasikan adanya ancaman seperti serangan denial-of-service (DoS), fuzzing, spoofing, atau replay attacks. Teknik deteksi ini sangat penting dalam konteks kendaraan otonom dan sistem kontrol kendaraan yang sangat bergantung pada jaringan komunikasi internal, seperti Controller Area Network (CAN) bus, di mana serangan terhadap jaringan ini dapat membahayakan keselamatan kendaraan dan pengendara.

Beberapa algoritma pembelajaran mesin dan teknik analisis data yang telah diterapkan untuk deteksi anomali dalam jaringan CAN termasuk K-Means clustering [5-13][23], Support Vector Machines (SVM) [9][14-18], serta pendekatan berbasis Deep Learning [19-22][24]. Algoritma K-Means, sebagai metode klasterisasi, bekerja dengan cara mengelompokkan data yang memiliki karakteristik serupa ke dalam grup atau klaster. Dengan memanfaatkan pendekatan ini, sistem deteksi anomali dapat mempelajari pola komunikasi normal dari jaringan kendaraan dan mengidentifikasi data baru yang tidak sesuai dengan pola tersebut, sehingga dapat mengindikasikan adanya anomali atau serangan. Selain itu, SVM digunakan untuk memisahkan data ke dalam kategori yang berbeda (misalnya, normal vs anomali) berdasarkan fitur-fitur tertentu yang diekstraksi dari data CAN. SVM dapat memberikan hasil yang sangat baik dalam situasi di mana data bersifat non-linear atau memiliki dimensi yang sangat tinggi. Sementara itu, teknik Deep Learning, khususnya Autoencoders atau Recurrent Neural Networks (RNN), digunakan untuk mendeteksi anomali yang lebih kompleks dan tidak dapat dengan mudah dikenali oleh algoritma tradisional.

Meskipun algoritma ini sudah terbukti efektif dalam mendeteksi berbagai jenis serangan dan anomali, salah satu tantangan utama adalah kemampuan untuk mendeteksi serangan yang sangat tersembunyi atau yang disamarkan dengan sangat baik. Dalam konteks keamanan, deteksi anomali berbasis analisis clock telah muncul sebagai pendekatan inovatif. Analisis ini memanfaatkan pola waktu antar pesan untuk mendeteksi perilaku yang tidak biasa, yang dapat mengindikasikan adanya serangan atau kerusakan sistem. Keunggulan pendekatan ini terletak pada kemampuannya untuk mendeteksi anomali secara real-time, sehingga memungkinkan respons cepat terhadap ancaman yang muncul. Dengan meningkatnya kompleksitas dan konektivitas kendaraan listrik, literatur ini mengeksplorasi berbagai pendekatan yang digunakan dalam deteksi anomali pada komunikasi CAN Bus dengan fokus utama pada analisis clock, serta tantangan dan peluang yang terkait dengan implementasi teknologi ini dalam lingkungan dunia nyata.

II. LANDASAN TEORI

A. CONTROLLER AREA NETWORK (CAN)

Controller Area Network (CAN) merupakan standar jaringan yang memanfaatkan protokol serial untuk pertukaran pesan antar perangkat. Diperkenalkan secara resmi pada tahun 2011 melalui ISO 11898-1:2011 [41], standar ini menyediakan spesifikasi

lengkap untuk mengatur koneksi antara Electronic Control Units (ECU). Karena keandalannya yang sangat baik, kinerja real-time yang konsisten, dan kemudahan dalam pemasangan kabel, CAN bus telah menjadi pilihan utama bagi produsen mobil besar di seluruh dunia [20]. CAN bus mengumpulkan aliran data cabang dari berbagai sistem kontrol inti kendaraan, seperti mesin, sistem transmisi, sistem bodi, serta peralatan listrik lainnya, yang semuanya saling terhubung dalam satu jaringan. Dengan cara ini, berbagai informasi penting terkait kinerja kendaraan, seperti suhu mesin, status baterai, kecepatan kendaraan, dan kondisi sistem rem, dapat dipertukarkan secara real-time antara ECU, memungkinkan pemantauan dan pengendalian kendaraan yang lebih efektif. Keuntungan lain dari penggunaan CAN bus adalah kemampuan untuk mengurangi kompleksitas kabel, karena semua ECU dapat terhubung melalui satu jaringan pusat, yang mempermudah perawatan dan meningkatkan keandalan sistem secara keseluruhan.

Gambar 1. Struktur Data Frame CAN

Start of Frame (SOF) digunakan untuk menginisialisasi bus ketika berada dalam keadaan idle, menandakan dimulainya transmisi pesan. Arbitration Field terdiri dari 11-bit yang berfungsi sebagai identitas pesan, dengan bit ke-12 sebagai RTR (Remote Transmission Request), yang membedakan pesan data dengan permintaan data [41]. Control Field mencakup dua bit yang disisihkan untuk cadangan dan Data Length Code (DLC) sepanjang 4-bit, yang menunjukkan panjang data yang dikirimkan, berkisar antara 0 hingga 8 byte. Data Field berisi data aktual yang akan ditransmisikan antar node, dengan panjang yang bervariasi sesuai dengan DLC [30]. CRC Field memastikan integritas data dengan menggunakan Cyclic Redundancy Check (CRC) untuk mendeteksi kesalahan transmisi [42]. Acknowledge Field terdiri dari bagian ACK dan ACK delimiter, yang masing-masing diwakili oleh satu bit untuk memberi sinyal apakah pesan diterima dengan benar [29]. Terakhir, End of Frame menandakan berakhirnya frame dengan menggunakan pengecekan tujuh bit recessive, memastikan frame telah selesai ditransmisikan. Semua field ini bekerja bersama untuk menjamin bahwa pesan dikirim secara terstruktur dan andal dalam jaringan CAN [48].

B. WAKTU ANTAR PESAN (INTER-ARRIVAL TIME)

Waktu antar pesan (Inter-Arrival Time) adalah selang waktu antara kedatangan dua pesan berturut-turut dalam sebuah sistem komunikasi, seperti Controller Area Network (CAN Bus). Dalam konteks CAN Bus, waktu antar pesan memiliki peran yang sangat penting karena memberikan gambaran tentang pola komunikasi antar Electronic Control Units (ECU) yang ada di dalam kendaraan atau sistem yang lebih besar. Sistem CAN digunakan dalam kendaraan untuk memungkinkan komunikasi antar berbagai ECU yang mengontrol berbagai fungsi kendaraan, seperti sistem penggerak, kontrol mesin, dan sistem keselamatan.

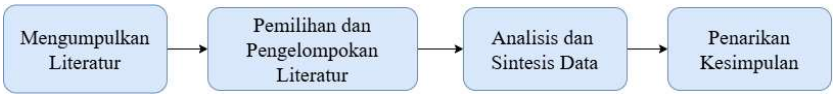
Pola waktu antar pesan pada CAN Bus biasanya konsisten karena banyak pesan yang dikirimkan secara periodik atau dalam interval yang telah ditentukan [53]. Misalnya, sensor kendaraan yang mengukur suhu mesin atau tekanan bahan bakar mengirimkan data secara berkala pada interval waktu tertentu. ECU yang mengontrol rem atau sistem pengereman otomatis juga mengirimkan data dengan frekuensi tetap untuk memastikan kelancaran komunikasi antar sistem. Keberlanjutan dan konsistensi waktu antar pesan ini adalah karakteristik utama dari komunikasi yang sah dalam jaringan CAN.

C. CLOCK SKEW

Jam komputer menggunakan kristal kuarsa untuk menjaga akurasi waktu, namun perbedaan fisik pada tingkat atom saat pembuatan menyebabkan variasi frekuensi osilasi, sehingga timbul ketidakakuratan waktu yang dikenal sebagai clock skew [51]. Clock skew diukur dalam satuan mikrodetik per detik (µs/s), yang sering disebut sebagai parts per million (ppm). Ini menggambarkan seberapa cepat dua jam yang tidak disinkronkan akan bergerak relatif satu sama lain, yang dapat digunakan untuk mengidentifikasi perbedaan dalam perangkat jaringan berdasarkan perilaku waktu mereka. Dalam pemanfaatan fitur clock skew pada Intrusion Detection System (IDS), waktu antar-transmisi (inter-transmission times) dari pesan yang secara periodik dikirimkan oleh suatu Electronic Control Unit (ECU) dipengaruhi oleh karakteristik unik dari clock skew-nya [52]. Clock skew menyebabkan setiap ECU memiliki pola waktu antar-transmisi pesan yang unik dan dapat diukur. Fenomena ini memberikan peluang untuk mengidentifikasi sumber pesan dengan memanfaatkan pola clock skew. Karena karakteristik clock skew cenderung stabil untuk setiap ECU, pola waktu antar-transmisi pesan yang dihasilkan oleh ECU tertentu akan konsisten. Dengan menganalisis pola tersebut, IDS dapat memverifikasi keaslian sumber pesan dan mendeteksi anomali, seperti adanya pesan palsu (spoofed messages) yang dikirimkan oleh ECU yang berbeda. Pendekatan ini menjadi penting dalam konteks keamanan, khususnya pada sistem komunikasi seperti Controller Area Network (CAN bus), di mana deteksi dini terhadap anomali sangat penting untuk mencegah serangan siber yang dapat memengaruhi integritas dan kinerja sistem.

III. METODE PENELITIAN

Penelitian ini menggunakan pendekatan deskriptif-kualitatif dengan tujuan utama mengkaji metode deteksi anomali berbasis analisis waktu dalam sistem komunikasi jaringan. Pendekatan ini bertujuan untuk memberikan pemahaman mendalam mengenai mekanisme deteksi anomali melalui analisis temporal dan dampaknya terhadap keamanan jaringan.



Gambar 2. Skema Penelitian

Gambar 2 merupakan skema dari alur penelitian ini. Pada tahapan awal peneliti melakukan pengumpulan literatur terkait berbagai pendekatan deteksi anomali pada komunikasi CAN Bus pada kendaraan listrik berbasis analisis clock. Literatur yang relevan dikumpulkan dari berbagai database akademik seperti Google Scholar, IEEE Xplore, SpringerLink, dan Science Direct. Pencarian dilakukan menggunakan kata kunci seperti "Anomaly Detection", "CAN Bus Anomaly Detection", "Clock based IDS CAN Bus". Artikel ilmiah yang dikumpulkan merupakan artikel yang dipublikasi dalam kurun waktu 9 tahun terakhir (2015-2024). Setelah pengumpulan, dilakukan penyaringan lebih lanjut.

TABEL I
KRITERIA INKLUSI DAN EKSKLUSI

Tahapan	Kriteria Inklusi	Kriteria Eksklusi
Tahap Inisiasi	- Studi yang menggunakan metode berbasis analisis waktu (seperti analisis delay, clock skew, timestamp). - Dipublikasikan pada tahun 2015 -2024. - Berasal dari prosiding atau jurnal - Ditulis dalam bahasa Indonesia atau bahasa inggris.	- Hanya membahas anomali berbasis payload atau konten data tanpa mempertimbangkan aspek waktu. - Dipublikasikan diluar tahun 2015 -2024 - Fokus penelitian bukan pada kendaraan listrik. - Tidak menggunakan pendekatan berbasis waktu
Tahap 1 – Berdasarkan judul dan abstrak	- Mengusulkan atau mengembangkan metode deteksi anomali pada CAN Bus berbasis waktu. - Menyediakan arsitektur, model, atau framework deteksi.	- Hanya membahas identifikasi serangan tanpa solusi deteksi. - Menggunakan teknik berbasis konten/payload saja tanpa aspek analisis waktu. - Studi tentang jaringan selain CAN Bus (misal: Ethernet)
Tahap 2 – Teks Penuh	- Menjelaskan metode deteksi anomali berbasis waktu secara detail (algoritma, eksperimen, atau hasil uji). - Mencantumkan hasil evaluasi atau validasi sistem deteksi pada CAN Bus kendaraan listrik.	- Tidak menyediakan informasi teknis mendetail tentang metode deteksi. - Penelitian berbasis simulasi tanpa validasi terhadap kendaraan listrik nyata atau data nyata.

Setelah tahap penyaringan, artikel diklasifikasikan ke dalam beberapa kategori topik sesuai dengan tema penelitian, yaitu bagaimana Pemanfaatan fitur waktu pada deteksi anomali, Dataset dan ekstraksi fitur berbasis waktu, Teknik Evaluasi model deteksi anomali serta Tantangan dan peluang lebih lanjut terkait deteksi anomali pada can bus kendaraan listrik berbasis analisis waktu. Pada Analisis dan Sintesis Data, peneliti melakukan eksplorasi menyeluruh terhadap setiap kategori yang telah diidentifikasi untuk menemukan tema-tema utama yang muncul dari data yang ada. Proses ini tidak hanya melibatkan identifikasi tema-tema tersebut, tetapi juga mengupas lebih dalam konteks dan makna yang terkandung dalam setiap tema. Peneliti berusaha memahami bagaimana setiap tema berkontribusi dalam memperkaya pemahaman tentang mekanisme dan efektivitas deteksi anomali pada CAN Bus yang berbasis analisis waktu. Selain itu, peneliti membandingkan temuan dari berbagai sumber literatur untuk mengidentifikasi pola-pola umum serta perbedaan yang signifikan antara pendekatan yang ada, sehingga bisa menarik kesimpulan yang lebih solid. Kemudian pada tahap akhir dilakukan penarikan kesimpulan berdasarkan analisis yang sudah dilakukan tentang deteksi anomali berbasis fitur waktu.

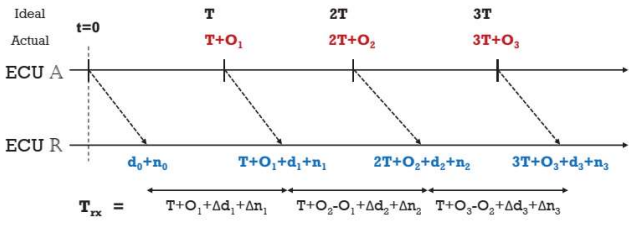
IV. HASIL DAN PEMBAHASAN

A. *EKSTRAKSI FITUR BERBASIS WAKTU*

Ekstraksi fitur berbasis waktu adalah proses identifikasi dan pemanfaatan informasi berbasis waktu dari suatu aliran data untuk menggambarkan karakteristik atau perilaku sistem yang sedang dianalisis. Dalam jaringan seperti Controller Area Network (CAN) pada kendaraan, fitur berbasis waktu digunakan untuk mengevaluasi pola komunikasi antar pesan yang dikirimkan oleh Electronic Control Units (ECUs). Proses ekstraksi fitur berbasis waktu ini sangat penting dalam mendeteksi anomali atau serangan yang dapat mempengaruhi integritas dan keandalan sistem kendaraan.

1) *PENGUKURAN INTERVAL WAKTU ANTAR PESAN*

Interval waktu antar pesan adalah salah satu fitur paling mendasar dalam jaringan CAN, di mana setiap pesan memiliki timestamp yang menunjukkan kapan pesan tersebut dikirim. Dengan mengukur interval antar pesan (misalnya, seberapa cepat atau lambat pesan-pesan tersebut dikirim), kita dapat mengidentifikasi pola komunikasi normal dan mengamati perubahan yang mungkin mengindikasikan adanya masalah atau serangan. Penelitian [42,54,56] memanfaatkan periodisitas pesan untuk mengekstrak dan memperkirakan clock skew pengirim, yang kemudian digunakan untuk fingerprint ECU pengirim tersebut.



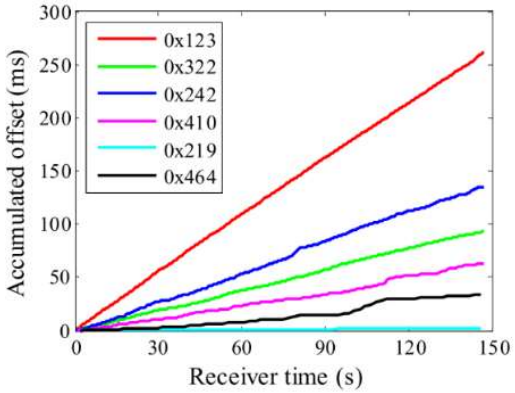
Gambar 3. Analisis Waktu Kedatangan

Pada Gambar 1, ECU A mengirimkan pesan secara periodik setiap T ms, yang seharusnya terjadi pada interval waktu yang tetap, yaitu T, 2T, 3T, dan seterusnya. Namun, pada kenyataannya, ECU R yang menerima pesan tersebut hanya memiliki informasi

waktu dari timestamp yang dimilikinya. Hal ini menyebabkan adanya clock skew yang akan menghasilkan sedikit pergeseran atau offset antara waktu pengiriman yang ideal dengan waktu pengiriman yang tercatat oleh ECU R [42]. Dalam hal ini, pengukuran terhadap interval waktu antara pesan-pesan yang diterima ECU R akan mengalami sedikit perubahan karena perbedaan antara jam ECU A dan ECU R. Persamaan $\mathbf{Tr_{x,i} = T + \Delta O_i + \Delta d_i + \Delta n_i}$ menggambarkan perhitungan interval kedatangan pesan pada sistem, seperti jaringan CAN. Dimana T adalah interval ideal antara pesan, ΔO_i adalah pergeseran jam pada ECU penerima, Δd_i adalah delay transmisi pesan, dan Δn_i adalah variasi atau gangguan dalam waktu kedatangan pesan [56]. Dengan menghitung $Tr_{x,i}$, sistem dapat mendeteksi penyimpangan waktu yang disebabkan oleh faktor-faktor seperti clock skew, delay jaringan, atau noise, yang dapat menunjukkan adanya serangan atau gangguan dalam jaringan. Analisis ini sangat penting untuk sistem deteksi intrusi yang mengandalkan pengamatan pola waktu pesan untuk mendeteksi anomali. Pendekatan berbasis waktu ini memberikan fondasi penting bagi sistem deteksi intrusi yang tidak bergantung pada isi pesan, melainkan pada perilaku waktu pengirimannya—menjadikannya pertahanan yang halus namun efektif terhadap potensi serangan siber.

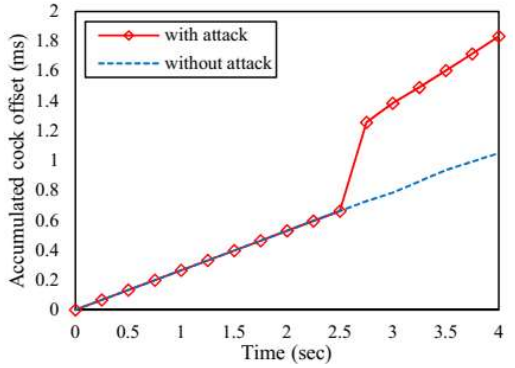
2) ANALISIS DISTRIBUSI WAKTU

Dengan memantau waktu antar pesan, kita dapat menggambarkan distribusi waktu pesan-pesan yang dikirimkan pada CAN bus. Jika terdapat anomali dalam distribusi ini—misalnya, pesan dikirim lebih cepat atau lebih lambat dari yang seharusnya—sistem dapat mengidentifikasi potensi masalah. Analisis distribusi waktu berfokus pada bagaimana waktu antar pesan dikirimkan dan diterima, serta mengidentifikasi perbedaan-perbedaan waktu (seperti clock skew) yang dapat menunjukkan anomali atau masalah dalam komunikasi antar ECU. Dalam konteks ini, analisis tersebut mengamati distribusi offset waktu antar pesan yang dikirim dan diterima, serta bagaimana perbedaan waktu tercermin dalam kemiringan garis pada grafik. Hal ini memberikan wawasan mengenai ketepatan dan konsistensi sinkronisasi waktu antar perangkat di jaringan CAN, yang penting untuk mendeteksi potensi masalah atau serangan. Salah satu tahapan analisis distribusi waktu dilakukan analisis hubungan antara akumulasi offset dan waktu penerima pesan dalam jaringan CAN, seperti yang dijelaskan dalam contoh salah satu kendaraan pada penelitian sebelumnya [42, 61].



Gambar 4. Hubungan antara Akumulasi Offset dan Waktu Penerima untuk Pesan-pesan pada Jaringan CAN [61]

Pada gambar di atas, setiap garis mewakili hubungan yang berbeda dari setiap pesan, dan kemiringan (*slope*) setiap garis menunjukkan *clock skew* dari ECU relatif yang terlibat. Clock skew ini mencerminkan perbedaan waktu antara jam ECU pengirim dan jam ECU penerima, yang dapat digunakan untuk menganalisis sinkronisasi waktu antar ECU dalam jaringan CAN. Selain pada data normal, analisis perbandingan hubungan antara akumulasi *offset* dan waktu penerima pesan dilakukan juga pada data yang terkontaminasi anomali atau intrusi dan data normal.



Gambar 5. Perbandingan Hubungan antara Akumulasi Offset dan Waktu Penerima untuk Pesan-Pesan pada Jaringan CAN pada Data Terkontaminasi Anomali dan Data Normal [42]

Grafik pada Gambar 3 menggambarkan bagaimana nilai offset jam yang terakumulasi berfluktuasi baik dalam kondisi normal (tanpa serangan) maupun ketika serangan DoS (*Denial of Service*) dilancarkan. Dalam kondisi normal, nilai offset jam biasanya berubah secara perlahan dan stabil, mencerminkan keakuratan komunikasi antar ECU dalam jaringan. Namun, ketika ECU Z melancarkan serangan DoS, terdapat perubahan yang sangat tajam dan tiba-tiba pada nilai offset jam yang terakumulasi, yang langsung bergerak ke arah positif. Pola perubahan akumulasi offset waktu bukan hanya merefleksikan performa sinkronisasi antar

ECU, tetapi juga dapat berfungsi sebagai indikator sensitif terhadap serangan siber seperti DoS. Dengan memanfaatkan perubahan kemiringan dan pola distribusi offset secara cermat, sistem deteksi dapat mengidentifikasi deviasi dari perilaku komunikasi normal, menjadikan analisis temporal sebagai komponen penting dalam strategi keamanan jaringan CAN yang responsif dan presisi.

B. EVALUASI MODEL DETEKSI ANOMALI

Model evaluasi penting untuk menilai sejauh mana model deteksi berbasis clock dapat secara akurat mendeteksi gangguan atau perubahan yang mencurigakan dalam waktu yang dikirimkan antar perangkat dalam jaringan. Tabel III merangkum beberapa model evaluasi yang digunakan untuk menilai kinerja sistem deteksi atau klasifikasi. Cross Validation digunakan untuk menguji model dengan membagi dataset menjadi beberapa subset untuk memastikan generalisasi model. F1-score menggabungkan precision dan recall untuk mengevaluasi keseimbangan antara keduanya, terutama pada dataset yang tidak seimbang. Confusion Matrix Evaluation memberikan gambaran yang lebih rinci tentang kinerja model dengan menghitung TP, FP, TN, dan FN untuk memperoleh metrik lain seperti akurasi dan sensitivitas. Average Deviation Error (ADE) mengukur kesalahan rata-rata dalam prediksi, yang sangat berguna dalam model prediksi berbasis waktu. Sedangkan False Alarm Rate (FAR) mengukur tingkat alarm palsu yang dihasilkan oleh sistem, yang penting untuk menghindari prediksi positif palsu. Secara keseluruhan, model-model evaluasi ini memberikan alat yang komprehensif untuk menilai dan membandingkan kinerja sistem deteksi intrusi atau klasifikasi berdasarkan berbagai metrik.

TABEL III
TEKNIK EVALUASI MODEL DETEKSI ANOMALI CAN BUS

No.	Metrik Evaluasi	Ref
1.	Cross Validation	[59]
2.	F1-score	[19], [53],[58], [59], [50]
3.	Confusion Matrix Evaluation	[35], [57], [60] [61], [55]
4.	Average Deviation Error (ADE)	[54]
5.	False Alarm Rate (FAR)	[56],[74]
6.	Missed Detection Rate (MDR)	[74]

C. PEMANFAATAN FITUR WAKTU DALAM DETEKSI ANOMALI

Pemanfaatan waktu dalam deteksi anomali merupakan aspek krusial dalam meningkatkan efektivitas dan akurasi sistem deteksi, terutama dalam sistem yang melibatkan data waktu nyata seperti pada sistem komunikasi kendaraan listrik atau jaringan IoT. Informasi waktu dapat memberikan konteks tambahan yang sangat berharga. Dengan memanfaatkan timestamp atau informasi waktu, algoritma deteksi anomali dapat mengidentifikasi pola yang tidak biasa atau peristiwa yang terjadi pada interval waktu tertentu, yang mungkin menunjukkan adanya gangguan atau ancaman. Misalnya, dalam konteks kendaraan listrik, perbedaan waktu antara pesan yang dikirim dan diterima pada sistem CAN bus dapat mengindikasikan masalah komunikasi atau bahkan potensi intrusi. Dengan demikian, pemanfaatan informasi waktu memungkinkan model deteksi anomali untuk lebih sensitif terhadap perubahan yang mungkin tidak tampak dalam analisis berbasis data statis, meningkatkan kemampuan sistem dalam mendeteksi masalah lebih cepat dan lebih akurat. Terdapat dua pendekatan deteksi anomali pada CAN bus berdasarkan waktu, yaitu pendekatan berbasis clock skew dan Inter-Arrival Time.

1) CLOCK SKEW SEBAGAI FITUR EKSTRAKSI

Clock skew mengacu pada perbedaan kecil dalam frekuensi clock antara perangkat dalam jaringan CAN Bus. Dalam kondisi normal, clock skew relatif stabil untuk setiap perangkat. Perubahan mendadak pada pola clock skew dapat mengindikasikan adanya manipulasi atau serangan pada jaringan. Salah satu pendekatan untuk mendeteksi anomali berdasarkan clock skew adalah analisis statistik. Metode ini memanfaatkan distribusi statistik dari clock skew untuk mengidentifikasi pola yang tidak biasa atau perubahan signifikan yang menunjukkan adanya potensi ancaman. Selain itu, time series analysis juga dapat digunakan untuk mempelajari perubahan dinamis dalam clock skew. Dengan menggunakan model time series, pola perubahan clock skew dapat dipelajari secara lebih rinci untuk mendeteksi fluktuasi yang tidak wajar, yang mungkin mencerminkan adanya manipulasi atau gangguan dalam sistem komunikasi. Pendekatan ini memungkinkan deteksi anomali yang lebih sensitif dan adaptif terhadap kondisi waktu nyata, meningkatkan keandalan dan respons sistem terhadap potensi ancaman.

X. Ying et al.[54] memperkenalkan serangan baru yang disebut cloaking attack dan memberikan analisis formal terhadap sistem deteksi intrusi (IDS) berbasis clock skew yang dirancang untuk mendeteksi serangan masquerade di Controller Area Network (CAN) pada kendaraan bermotor. Serangan cloaking ini merupakan upaya penyerang untuk menyembunyikan identitas asli mereka dengan memanipulasi waktu antar-transmisi pesan dari pesan palsu yang dikirimkan, dengan cara menambahkan penundaan yang terkontrol. Tujuannya adalah untuk meniru clock skew tertentu, sehingga menyamarkan pola waktu yang tidak biasa dan menghindari deteksi oleh IDS yang memanfaatkan clock skew untuk mendeteksi intrusi. Hasil eksperimen menunjukkan bahwa serangan cloaking efektif dalam melewati kedua IDS yang kami uji, yaitu IDS berbasis SOTA dan NTP. Kami juga membandingkan kurva probabilitas keberhasilan serangan yang diprediksi dengan kurva yang diperoleh dari eksperimen lapangan. Temuan kami menunjukkan bahwa prediksi yang kami buat memiliki kesalahan rata-rata yang sangat kecil, yaitu 3,0% untuk IDS berbasis SOTA dan 5,7% untuk IDS berbasis NTP. Ini menunjukkan bahwa model formal yang kami kembangkan dapat memberikan prediksi yang akurat mengenai keberhasilan serangan, dan oleh karena itu dapat digunakan untuk lebih memahami potensi risiko yang terkait dengan serangan cloaking dalam sistem CAN.

Sebuah sistem deteksi intrusi berbasis anomali yang disebut Clock-based IDS (CIDS) pada penelitian [56]. Dengan menggunakan algoritma Recursive Least Squares (RLS) dilakukan menganalisis sidik jari yang diperoleh ini kemudian digunakan

untuk membangun dasar perilaku jam ECU. Berdasarkan dasar perilaku ini, CIDS menggunakan Cumulative Sum (CUSUM) untuk mendeteksi perubahan abnormal pada kesalahan identifikasi yang merupakan tanda jelas adanya intrusi. Evaluasi menunjukkan bahwa Clock-based IDS (CIDS) mampu mendeteksi berbagai jenis intrusi pada jaringan kendaraan dengan tingkat false-positive yang sangat rendah, yaitu 0,055%.

J. Zhou et al. [59] mengembangkan sebuah IDS berbasis clock skew. Dimana proses estimasi clock skew dalam pendekatan kami hanya bergantung pada pengukuran waktu dari satu frame CAN tunggal, sehingga gangguan dari lapisan data-link dapat dihindari. Penerapan pendekatan ambang batas dinamis secara signifikan meningkatkan False Positive Rate (FPR) pada semua algoritma klasifikasi. Pada SVM, FPR turun dari 7.78% menjadi 2.16% saat jumlah sampel data 200 dan berkurang sekitar 16.59% saat jumlah sampel data 50. Selain NB, perubahan FPR pada algoritma lain relatif kecil meskipun jumlah sampel data bervariasi, menunjukkan FPR yang stabil dan rendah bahkan untuk data sample kecil. Pada NB, FPR menurun seiring peningkatan jumlah sampel data dan stabil mulai N=200. Selain itu, tingkat kecurigaan pada semua algoritma tetap rendah dan stabil.

Penelitian berbasis clock drift dengan mengadopsi algoritma CUSUM (Cumulative Sum) untuk mendeteksi perubahan kesalahan identifikasi berdasarkan akumulasi penyimpangan dilakukan oleh H. Ji et al. [61]. Algoritma CUSUM berbasis drift jam memiliki keterbatasan, seperti deteksi pesan palsu yang lemah dan tingginya false positive pada data tidak stabil. Meskipun terus dioptimalkan, kasus false negative tetap tidak terhindarkan. Selain itu, deteksi pesan aperiodik sulit dilakukan karena sulitnya memperoleh ECU dengan clock skew tetap pada kendaraan nyata.

Berdasarkan kajian dari berbagai penelitian sebelumnya, dapat disimpulkan bahwa clock skew merupakan fitur waktu yang relatif stabil dan unik dari setiap ECU dalam jaringan CAN, sehingga potensial digunakan untuk mendeteksi anomali dan melakukan fingerprinting perangkat. Namun, keberhasilan serangan seperti cloaking attack menunjukkan bahwa clock skew juga rentan dimanipulasi oleh penyerang canggih untuk menghindari deteksi. Metode deteksi berbasis analisis statistik dan time series, seperti Recursive Least Squares (RLS) dan Cumulative Sum (CUSUM), telah menunjukkan efektivitas dalam mengenali perubahan abnormal dalam pola clock skew, dengan tingkat false positive yang rendah dalam banyak kasus. Meskipun demikian, tantangan tetap ada dalam menghadapi kondisi nyata, seperti pesan aperiodik, noise tinggi, dan keterbatasan sumber daya komputasi untuk sistem real-time. Oleh karena itu, pengembangan Intrusion Detection System (IDS) berbasis clock skew perlu mempertimbangkan ketepatan model, efisiensi komputasi, serta ketahanan terhadap manipulasi temporal, guna memastikan sistem keamanan kendaraan yang adaptif dan tangguh terhadap evolusi ancaman siber.

2) WAKTU ANTAR PESAN (INTER-ARRIVAL TIME) SEBAGAI FITUR EKSTRAKSI

Waktu antar pesan merupakan parameter krusial dalam komunikasi Controller Area Network (CAN) Bus, yang menggambarkan interval antara pengiriman pesan dari satu perangkat ke perangkat lain. Setiap ECU dalam jaringan CAN diharapkan mengikuti pola waktu tertentu dalam pengiriman pesan, yang bisa dipengaruhi oleh berbagai faktor, termasuk kondisi lalu lintas data dan prioritas pesan. Penyimpangan dari pola waktu antar pesan yang diharapkan dapat mengindikasikan adanya serangan, seperti injection attack atau replay attack, yang berusaha mengganggu komunikasi antar ECU. Salah satu pendekatan untuk mendeteksi penyimpangan ini adalah dengan menggunakan Threshold-Based Detection, di mana sistem menetapkan ambang batas waktu antar pesan yang normal. Ketika waktu antar pesan melebihi atau kurang dari batas tersebut secara signifikan, maka sistem akan menandai hal ini sebagai potensi intrusi.

D. Stabili et al. [53] mengusulkan algoritma yang dapat mendeteksi pesan-pesan yang hilang dari bus CAN kendaraan akibat masalah serangan bus-off. Serangan bus-off terjadi ketika mikrokontroler dalam jaringan CAN dipaksa untuk memasuki mode bus-off, sehingga tidak dapat lagi berpartisipasi dalam komunikasi jaringan. Dalam eksperimen ini, serangan tersebut disimulasikan dengan cara menghapus pesan-pesan dari jejak-jejak CAN yang valid, yang sebelumnya telah direkam dari kendaraan berlisensi yang tidak dimodifikasi. Evaluasi eksperimental yang kami lakukan terhadap usulan algoritma ini menunjukkan hasil yang menggembirakan. Algoritma yang diusulkan terbukti mampu mendeteksi pesan yang hilang dengan akurasi tinggi, mencapai deteksi hampir sempurna dengan nilai F-score yang mendekati 1.0 pada berbagai pengujian. Keunggulan utama dari algoritma ini adalah kemampuannya untuk mendeteksi hilangnya pesan secara efektif tanpa terganggu oleh fluktuasi jaringan CAN yang wajar. Selain itu, algoritma kami dapat beradaptasi dengan berbagai jenis serangan bus-off, bahkan ketika serangan dilakukan dalam skenario yang lebih kompleks, seperti dalam kendaraan dengan arsitektur jaringan yang lebih dinamis.

Selain Threshold-Based Detection, Machine Learning dan Statistic Models, seperti Long Short-Term Memory (LSTM), dapat digunakan untuk mempelajari dan memahami pola waktu antar pesan secara lebih adaptif. Algoritma LSTM memiliki kemampuan untuk menangkap hubungan jangka panjang dalam data waktu yang dapat membantu mendeteksi perubahan pola yang lebih halus dan tidak terduga, memberikan solusi yang lebih fleksibel dan akurat dalam deteksi anomali pada jaringan CAN.

Pendekatan deteksi anomali berbasis CNN (Convolutional Neural Network) dan GRU (Attention-Based Gated Recurrent Unit) digunakan oleh A. R. Javed et al. [19]. CNN digunakan untuk mengekstrak fitur spasial dari data, sementara GRU dengan mekanisme perhatian mempelajari pola temporal dan memberikan bobot lebih besar pada sekuens relevan. Output diklasifikasikan melalui lapisan fully connected dengan aktivasi sigmoid atau softmax. Model dilatih menggunakan dataset CAN dengan metrik evaluasi seperti Accuracy, Recall, Precision, dan F1 Score, lalu dibandingkan dengan pendekatan baseline. Pendekatan ini dapat diimplementasikan sebagai sistem pendeteksian intrusi real-time tanpa mengubah protokol CAN, meningkatkan keamanan kendaraan dengan deteksi serangan yang lebih akurat dan respons cepat.

Peneliti [35] mengusulkan Long Short-Term Memory (LSTM) untuk mendeteksi anomali pada jaringan CAN. Setelah dilatih, sistem kami mampu mendeteksi anomali secara real-time dengan penggunaan sumber daya yang minimal. Hasil penelitian kami menunjukkan bahwa mesin deteksi anomali yang diusulkan berhasil mendeteksi anomali dengan akurasi lebih dari 98% dan tingkat false-positive antara 1% hingga 2%. Kinerja ini menunjukkan efektivitas tinggi dalam mengenali perilaku abnormal dalam jaringan CAN kendaraan, sambil meminimalkan kesalahan deteksi yang dapat mengganggu sistem.

Subir Halder et al. [42] mengusulkan Clock Offset-based Intrusion Detection System (COIDS) menggunakan metode Cumulative Sum (CUSUM) untuk mendeteksi deviasi abnormal pada clock offset. CUSUM adalah metode yang efektif untuk mendeteksi perubahan bertahap atau tiba-tiba dalam data yang memerlukan pemantauan terus-menerus. Jika deviasi clock offset melebihi ambang batas yang tidak terduga, baik positif maupun negatif. COIDS secara otomatis menganggapnya sebagai indikasi intrusi. Ini adalah sinyal bahwa komunikasi antara ECUs mungkin telah dimanipulasi atau disusupi oleh pihak yang tidak berwenang. COIDS terbukti lebih cepat dalam mendeteksi intrusi dibandingkan dengan solusi deteksi intrusi lainnya yang ada saat ini. Keunggulan ini memberikan keuntungan besar dalam aplikasi dunia nyata, di mana deteksi intrusi yang cepat dan tepat sangat penting untuk menghindari kerusakan lebih lanjut pada sistem kendaraan. Dengan demikian, COIDS tidak hanya menawarkan pendekatan yang lebih tepat dan efisien untuk mendeteksi serangan pada CAN bus, tetapi juga memberikan solusi yang lebih responsif dan handal dalam menjaga keamanan kendaraan modern.

Zixiang Bi et al. [50] mengusulkan sebuah metode deteksi intrusi inovatif yang berbasis pada matriks transfer pesan dan waktu untuk mengatasi berbagai tantangan yang dihadapi dalam deteksi intrusi kendaraan bermotor modern, khususnya pada Electronic Control Unit (ECU). Matriks transfer pesan dan waktu bekerja dengan memanfaatkan pola komunikasi antar pesan dalam jaringan CAN dan interval waktu antar transmisi pesan tersebut, yang dapat mengungkapkan adanya penyimpangan atau anomali yang mengindikasikan serangan. Metode ini tidak hanya menawarkan akurasi tinggi dan efisiensi sumber daya tetapi juga keunggulan dalam skala besar, menjadikannya solusi yang sangat ideal untuk diterapkan pada sistem CAN kendaraan masa depan. Dengan kemampuan deteksi real-time dan ketahanan terhadap serangan yang semakin kompleks, pendekatan ini berpotensi menjadi fondasi untuk pengembangan sistem keamanan kendaraan yang lebih canggih dan handal.

Sebuah metode baru diperkenalkan oleh Seyoung Lee et al. [55] bernama Transmission-resuming Time-based IDS (TTIDS) bekerja dengan mendeteksi serangan masquerade pada jaringan Controller Area Network (CAN) dengan memanfaatkan informasi waktu dan pola periodik transmisi pesan pada Electronic Control Units (ECUs) kendaraan. Dimana hasil eksperimen secara keseluruhan menunjukkan tingkat kesalahan yang rendah, dengan tingkat false positive sebesar 0,213% dan tingkat false negative sebesar 0,027%. Kesimpulannya, TTIDS mampu mendeteksi serangan masquerade secara efektif, memberikan solusi yang lebih handal dalam menghadapi serangan yang sulit dideteksi oleh metode deteksi yang ada.

TABEL II
PENELITIAN TERKAIT DETEKSI ANOMALI BERBASIS WAKTU

No.	Ref	Tahun	Metode	Log Datasheet	Hasil
1.	[56]	2016	Clock-based IDS (CIDS), Recursive Least Squares (RLS), Cumulative Sum (CUSUM)	Toyota Camry 2010 [62], Dodge Ram Pickup 2010 - Daily [63]	Recall : 97% FAR : 0.055%
2.	[61]	2018	Clock Drift, Cumulative Sum (CUSUM)	*Real Data capture*	TPR : 100% FPR : 7.4 %
3.	[60]	2018	ARIMA, Z-score, Time-defined window approach	*Real Data capture*	Sensitifitas: • ARIMA: ~0.8 • Z-score: ~0.8 • Supervised: ~0.95 Specificity: • ARIMA: ~0.95 • Z-score: ~0.9 • Supervised: ~0.8 Akurasi: • ARIMA: ~0.9 • Z-score: ~0.85 • Supervised: ~0.82
4.	[54]	2019	Clock Skew-based IDS	*Real Data capture*	-
5.	[53]	2019	Inter-Arrival Time Analysis	VTC2019Fall Dataset (2019) [64]	F-measure : 0:99964
6.	[58]	2019	Bit-time-based Intrusion Detection and Attacker Identification	*Real Data capture*	Akurasi : 99%
7.	[35]	2020	Long Short-Term Memory (LSTM)	*Real Data capture*	Akurasi : 98%
8.	[42]	2020	Clock Offset-based Intrusion Detection System (COIDS), Cumulative Sum (CUSUM)	CAN Dataset for intrusion detection (OTIDS) 2018 [65]	-
9.	[57]	2020	Recurring patterns and time interval of individual CAN ID	Mattia Zago et al. ReCAN Data [66]	FPR : 0.2% - 5.2%

10.	[19]	2021	CANintelliIDS	CAN Dataset for intrusion detection (OTIDS) 2018 [65]	Akurasi : 93.79% - 94.38%
11.	[59]	2021	Clock-Based Sender Identification and Attack Detection	*Real Data capture*	Akurasi > 99.7%
12	[72]	2021	Signature-Based Intrusion Detection System (IDS) for In-Vehicle CAN Bus Network	*Real Data capture*	Drop attack : 100% Replay attack : 98.2%. tempering attack : 66.2%.
13.	[50]	2022	Intrusion detection method based on the message and time transfer matrix	*Real Data capture*	Skema terbaik : Message & time transfer matrix Akurasi deteksi DoS : 100% Akurasi deteksi Fuzzy Attack : 99% Akurasi deteksi Ulterior Fuzzy Attack : 95% Akurasi deteks Replay Attack : 93%
14.	[55]	2022	Transmission-resuming Time-based IDS (TTIDS)	*Real Data capture*	FPR : 0.213% FNR : 0.027%
15.	[74]	2024	Quantile L1 Regression	CAN Dataset for intrusion detection (OTIDS) 2018 [65]	FAR : 0% MDR : 1.29%

Peneliti [57] mengusulkan sebuah metode hibrida menggunakan pola berulang dan interval waktu dari setiap CAN ID untuk mendeteksi anomali. Dimana Sistem ini tidak memerlukan informasi khusus tentang fungsi dari masing-masing pesan CAN serta tidak membutuhkan perubahan atau modifikasi pada protokol CAN yang ada, sehingga dapat diterapkan tanpa perlu pemahaman mendalam terhadap fungsi spesifik dari setiap ID CAN dan menjadi solusi yang praktis. Hasil eksperimen menunjukan FPR meningkat seiring dengan bertambahnya ukuran jendela. Hal ini menunjukkan bahwa pendekatan berbasis pola berulang cenderung menghasilkan jumlah false positive yang konstan di semua skenario.

Sebuah sistem deteksi intrusi dengan memantau waktu bit dari setiap pesan yang diterima di bus CAN diusulkan oleh Jia Zhou et al. [58]. Jika ada penyimpangan signifikan dari profil normal ECU yang teridentifikasi, sistem menandainya sebagai potensi intrusi. BTMonitor menggunakan pola waktu bit unik untuk menentukan asal pesan yang mencurigakan. Dengan demikian, sistem dapat mengidentifikasi ECU yang berperilaku tidak normal atau ECU palsu yang disisipkan oleh penyerang. Setiap perangkat pada bus memiliki tanda waktu bit tertentu yang membuatnya dapat diidentifikasi, sehingga penyerang sulit menyembunyikan identitasnya.

Pendekatan berbasis jendela waktu digunakan pada penelitian [60]. Penelitian ini menguji tiga metode deteksi berbeda yaitu ARIMA, Z-score, dan ambang batas terawasi yang menggunakan jendela waktu terdefinisi dan membandingkan kinerjanya dalam deteksi anomali waktu pesan CAN serta mengeksplorasi bagaimana evaluasi metode deteksi anomali waktu CAN ini, atau metode potensial lainnya, memerlukan pertimbangan terhadap akurasi, spesifisitas, dan sensitivitas. Pendekatan Unsupervised (seperti ARIMA dan Z-score) menawarkan solusi yang kemungkinan lebih independen terhadap analisis spesifik dari CAN yang digunakan.

Penelitian [72] menggunakan pendekatan berbasis analisis interval waktu kedatangan pesan dengan menggunakan periode transmisi pesan dan worst-case response time (WCRT). Interval waktu kedatangan pesan dengan ID tertentu mencerminkan karakteristik waktu yang spesifik, yang seharusnya konsisten dalam kondisi normal. Peneliti memilih lima tanda (signatures) berikut untuk mendeteksi serangan manipulasi (tamper), pemutaran ulang (replay), dan penghilangan (drop): ID, interval waktu, korelasi, amplitudo perubahan konteks, dan rentang nilai.

Maliha et al. [74] mengusulkan model deteksi intrusi berbasis anomali dua tingkat yang melacak penyimpangan jangka pendek dan jangka panjang dalam ruang laten deret waktu, menciptakan apa yang disebut sebagai 'ruang laten berstatus' (stateful latent space). Model ini membantu mengidentifikasi serangan dengan mendefinisikan batasan ruang laten berstatus yang baik, yang menetapkan kriteria untuk deteksi serangan. Aspek unik dari model yang diusulkan adalah penggunaan masalah optimisasi multi-objektif berbasis preferensi untuk menemukan hyperparameter yang optimal. Optimisasi ini menyeimbangkan tujuan keamanan utama seperti jumlah alarm palsu, waktu deteksi, dan tingkat deteksi yang terlewat, memastikan bahwa sistem deteksi intrusi efektif dan efisien.

Waktu antar pesan pada jaringan CAN merupakan indikator penting untuk mendeteksi anomali atau serangan terhadap sistem komunikasi kendaraan. Metode ini mudah diimplementasikan tanpa memerlukan perubahan pada protokol CAN yang ada, memberikan keuntungan praktis untuk kendaraan yang sudah ada. Berbagai pendekatan telah dikembangkan untuk memanfaatkan pola waktu ini, mulai dari metode threshold-based detection hingga model cerdas berbasis machine learning seperti LSTM, CNN-GRU, dan attention-based models, yang mampu mendeteksi anomali secara adaptif dan real-time. Penelitian juga menunjukkan efektivitas algoritma seperti CUSUM dan metode berbasis matriks waktu dalam mengidentifikasi penyimpangan temporal akibat serangan seperti bus-off dan masquerade attack. Meskipun hasil evaluasi menunjukkan tingkat akurasi tinggi dan false positive rendah, tantangan seperti deteksi pesan aperiodik, efisiensi sumber daya, dan generalisasi ke berbagai kondisi kendaraan tetap menjadi fokus pengembangan selanjutnya.

TABEL III
TABEL PERBANDINGAN PENDEKATAN BERBASIS CLOCK SKEW DAN PENDEKATAN BERBASIS WAKTU ANTAR PESAN

Aspek	Pendekatan Berbasis Clock Skew	Pendekatan Berbasis Waktu Antar Pesan (Inter-Arrival Time)
Fokus Deteksi	Penyimpangan dalam sinkronisasi waktu antar ECU.	Penyimpangan dalam interval waktu antar pesan.
Keunggulan Utama	Deteksi terhadap serangan yang memanipulasi sinkronisasi waktu.	Deteksi pola komunikasi abnormal dengan kecepatan respons tinggi.
Kemampuan Adaptasi	Mampu mendeteksi serangan yang mencoba menyembunyikan manipulasi waktu.	Lebih fleksibel dan adaptif dalam mendeteksi perubahan kecil dalam pola waktu antar pesan.
Kecepatan Deteksi	Deteksi cepat terhadap penyimpangan besar dalam sinkronisasi jam.	Deteksi cepat terhadap perubahan interval waktu antar pesan.
Tantangan	Rentan terhadap serangan yang menyinkronkan jam antar perangkat.	Kesulitan mendeteksi fluktuasi normal dalam trafik jaringan yang sangat tinggi.
Sumber Daya yang Dibutuhkan	Mungkin memerlukan pengelolaan sinkronisasi waktu yang lebih kompleks.	Cenderung lebih ringan dan bisa diterapkan dengan sedikit perubahan.

D. TANTANGAN

Deteksi anomali berbasis waktu berfokus pada menganalisis interval atau pola waktu pengiriman pesan yang diterima dalam sistem. Setiap pesan yang dikirim dalam jaringan biasanya disertai dengan timestamp, yang mencatat waktu pengirimannya. Dengan menganalisis timestamp dan interval antar pesan, sistem dapat mendeteksi jika ada pesan yang dikirim lebih cepat atau lebih lambat dari biasanya, yang dapat menjadi indikasi adanya serangan seperti Denial of Service (DoS) atau Replay Attacks. Namun terdapat beberapa tantangan yang dihadapi dalam pendekatan ini. Pertama, ketergantungan parameter pada periodisitas pesan menjadi masalah utama. Pendekatan dengan analisis waktu bekerja dengan mengandalkan periodisitas pesan untuk mengidentifikasi ketidakwajaran dalam perilaku jam, mengasumsikan bahwa setiap pesan dikirim dengan interval waktu yang teratur [73]. Namun, dalam jaringan dengan pesan yang dikirim secara aperiodik, seperti yang sering terjadi pada jaringan CAN, ketergantungan pada periodisitas ini dapat menyebabkan deteksi yang tidak akurat atau bahkan gagal dalam mengidentifikasi serangan, seperti serangan spoofing atau replay attacks, yang memanfaatkan pengiriman pesan yang tidak teratur. Hal ini menunjukkan keterbatasan pendekatan berbasis analisis waktu dalam mendeteksi intrusi pada jaringan yang tidak sepenuhnya terstruktur.

Deteksi anomali berbasis analisis waktu sangat terkait dengan keterbatasan waktu nyata pada sistem CAN kendaraan, karena sistem ini mengharuskan pengolahan data secara langsung tanpa menyebabkan penundaan yang mengganggu kinerja kendaraan [75]. Teknik ini memanfaatkan pola dan interval waktu pesan antar ECU untuk mendeteksi anomali yang mungkin menunjukkan adanya serangan, seperti replay, spoofing, atau DOS. Karena pengolahan data harus cepat, deteksi anomali harus dilakukan dengan efisien agar tidak menambah latensi yang dapat mempengaruhi respons sistem kendaraan, seperti pengaktifan pengereman atau perubahan arah. Dengan demikian, deteksi anomali berbasis waktu harus dapat memastikan keamanan tanpa mengorbankan performa real-time kendaraan.

E. PELUANG

Pendekatan berbasisi analisis waktu, terutama CIDS menawarkan pendekatan yang sangat efektif dan fleksibel dalam mendeteksi intrusi dan menjaga integritas sistem komunikasi kendaraan, yang sangat penting dalam menghadapi ancaman di era kendaraan terhubung dan otomatis [56]. Karena CIDS memanfaatkan sifat periodik dari pesan-pesan yang dikirimkan dalam jaringan kendaraan. Setiap ECU biasanya mengirimkan pesan secara periodik dengan interval waktu yang teratur, yang dapat diamati oleh penerima pesan. Dengan memonitor interval waktu antar pesan ini, CIDS mampu memperkirakan *clock skew* antara transmitter dan receiver tanpa memerlukan timestamp eksplisit dalam pesan. Selain itu Keunggulan utama dari pendekatan *CIDS (Clock Skew Detection System)* adalah kemampuannya untuk mendeteksi intrusi tanpa bergantung pada informasi pengirim pesan yang biasanya tidak ada dalam protokol CAN [53]. Dalam protokol CAN, pesan-pesan yang dikirimkan tidak menyertakan identitas pengirimnya, sehingga serangan yang bertujuan untuk menyamar sebagai pengirim sah, seperti serangan masquerade, sulit untuk dideteksi. CIDS mengatasi kelemahan ini dengan memanfaatkan informasi tentang frekuensi pesan dan pola waktu pengiriman pesan untuk mengidentifikasi fingerprint dari pengirim, yang bersifat unik bagi setiap ECU dalam kendaraan.

V. KESIMPULAN

Penelitian ini menunjukkan bahwa deteksi anomali berbasis analisis waktu dalam jaringan CAN Bus, menggunakan teknik seperti Clock Skew Analysis dan Inter-Arrival Time Analysis, sangat efektif dalam mendeteksi berbagai jenis serangan di kendaraan terhubung dan otonom, termasuk spoofing, replay attacks, dan DoS. Teknik ini mampu mengidentifikasi perubahan pola komunikasi yang tidak wajar dengan efisiensi tinggi dan tingkat false positive yang rendah. Meskipun serangan dapat disembunyikan melalui manipulasi waktu dan pola pengiriman pesan, metode berbasis waktu memberikan sensitivitas yang kuat terhadap perubahan tersebut, menjadikannya alat yang andal dalam mengidentifikasi potensi ancaman dalam sistem kendaraan modern. Berikut ringkasan

Pendekatan berbasis clock skew lebih efektif dalam mendeteksi serangan yang berfokus pada manipulasi waktu antar perangkat, seperti MITM dan serangan replay. Namun, pendekatan ini lebih sensitif terhadap perbedaan sinkronisasi jam dan bisa kurang efektif jika penyerang dapat menyinkronkan jam dengan baik. Pendekatan berbasis waktu antar pesan lebih efektif dalam mendeteksi perubahan pola komunikasi yang mencurigakan, seperti serangan spoofing, dengan sensitivitas yang tinggi terhadap fluktuasi waktu antar pesan. Meskipun begitu, pendekatan ini bisa terhambat oleh fluktuasi jaringan yang alami dan sulit mendeteksi serangan yang sangat terstruktur. Sebagai validasi, beberapa metode deteksi telah diuji pada penelitian sebelumnya, seperti algoritma Cumulative Sum (CUSUM) yang efektif untuk mendeteksi perubahan bertahap dalam offset waktu, serta aplikasi Long Short-Term Memory (LSTM) dan Convolutional Neural Networks (CNN) yang mampu mendeteksi pola serangan yang lebih kompleks dan tersembunyi dalam data waktu nyata. Eksperimen menunjukkan bahwa kombinasi teknik ini memberikan hasil yang menggembirakan dalam hal akurasi deteksi serangan dan kecepatan respons, bahkan dalam skenario yang melibatkan perubahan waktu yang cepat atau serangan yang lebih tersembunyi. Namun, tantangan yang signifikan tetap ada terkait dengan deteksi serangan yang lebih tersembunyi, termasuk serangan masquerade atau cloaking attack, di mana penyerang berusaha menyamarkan identitas mereka dengan memanipulasi waktu pengiriman pesan.

Meskipun algoritma pembelajaran mesin, seperti Reinforcement Learning, mampu secara adaptif mempelajari pola serangan baru dan meningkatkan ketahanan terhadap ancaman yang berkembang, tantangan penerapannya dalam skala besar tetap ada, terutama dalam pengolahan data real-time. Pendekatan berbasis Edge Computing menawarkan solusi yang menjanjikan, memungkinkan analisis data secara lokal tanpa membebani jaringan atau sumber daya kendaraan, serta memungkinkan respons cepat dalam deteksi dan mitigasi ancaman di lapang an. Selain itu, pengembangan sistem deteksi anomali ini berpotensi diperluas ke arah ekosistem transportasi cerdas, memperkuat keamanan komunikasi antara kendaraan dan infrastruktur jalan raya (V2I), yang akan menjadi fondasi penting untuk transportasi masa depan yang lebih aman dan efisien.

KONFLIK KEPENTINGAN

Penulis menyatakan bahwa tidak terdapat konflik kepentingan dalam hasil penelitian ini.

REFERENSI

[1] Bari, B.S., Yelamarthi, K., Ghafoor, S. Intrusion Detection in Vehicle Controller Area Network (CAN) Bus Using Machine Learning: A Comparative Performance Study. Sensors 2023, 23, 3610. https://doi.org/10.3390/s23073610.
[2] T. C. M. Dönmez, "Anomaly Detection in Vehicular CAN Bus Using Message Identifier Sequences," in IEEE Access, vol. 9, pp. 136243-136252, 2021, doi: 10.1109/ACCESS.2021.3117038.
[3] Q. Luo and J. Liu, "Wireless Telematics Systems in Emerging Intelligent and Connected Vehicles: Threats and Solutions," in IEEE Wireless Communications, vol. 25, no. 6, pp. 113-119, December 2018, doi: 10.1109/MWC.2018.1700364.
[4] C. Wang, Z. Zhao, L. Gong, L. Zhu, Z. Liu and X. Cheng, "A Distributed Anomaly Detection System for In-Vehicle Network Using HTM," in IEEE Access, vol. 6, pp. 9091-9098, 2018, doi: 10.1109/ACCESS.2018.2799210.
[5] X. Zhao and W. Zhang, "An Anomaly Intrusion Detection Method Based on Improved K-Means of Cloud Computing," 2016 Sixth International Conference on Instrumentation & Measurement, Computer, Communication and Control (IMCCC), Harbin, China, 2016, pp. 284-288, doi: 10.1109/IMCCC.2016.108.
[6] Z. Wang, Y. Zhou and G. Li, "Anomaly Detection by Using Streaming K-Means and Batch K-Means," 2020 5th IEEE International Conference on Big Data Analytics (ICBDA), Xiamen, China, 2020, pp. 11-17, doi: 10.1109/ICBDA49040.2020.9101212.
[7] R. Kumari, Sheetanshu, M. K. Singh, R. Jha and N. K. Singh, "Anomaly detection in network traffic using K-mean clustering," 2016 3rd International Conference on Recent Advances in Information Technology (RAIT), Dhanbad, India, 2016, pp. 387-393, doi: 10.1109/RAIT.2016.7507933.
[8] Maazalahi, M., Hosseini, S. K-means and meta-heuristic algorithms for intrusion detection systems. Cluster Comput 27, 10377–10419 (2024). https://doi.org/10.1007/s10586-024-04510-7.
[9] E. H. Budiarto, A. Erna Permanasari and S. Fauziati, "Unsupervised Anomaly Detection Using K-Means, Local Outlier Factor and One Class SVM," 2019 5th International Conference on Science and Technology (ICST), Yogyakarta, Indonesia, 2019, pp. 1-5, doi: 10.1109/ICST47872.2019.9166366.
[10] K. Peng, V. C. M. Leung and Q. Huang, "Clustering Approach Based on Mini Batch Kmeans for Intrusion Detection System Over Big Data," in IEEE Access, vol. 6, pp. 11897-11906, 2018, doi: 10.1109/ACCESS.2018.2810267.
[11] Ravale, Ujwala, Nilesh Marathe, and Puja Padiya. "Feature selection based hybrid anomaly intrusion detection system using K means and RBF kernel function." Procedia Computer Science 45 (2015): 428-435.
[12] E. Khaledian, S. Pandey, P. Kundu and A. K. Srivastava, "Real-Time Synchrophasor Data Anomaly Detection and Classification Using Isolation Forest, KMeans, and LoOP," in IEEE Transactions on Smart Grid, vol. 12, no. 3, pp. 2378-2388, May 2021, doi: 10.1109/TSG.2020.3046602.
[13] W. O. K. Putra, Y. Purwanto and F. Y. Suratman, "Modified K-means algorithm using timestamp initialization in sliding window to detect anomaly traffic," 2015 International Conference on Control, Electronics, Renewable Energy and Communications (ICCEREC), Bandung, Indonesia, 2015, pp. 19-23, doi: 10.1109/ICCEREC.2015.7337042.
[14] S. D. D. Anton, S. Sinha and H. Dieter Schotten, "Anomaly-based Intrusion Detection in Industrial Data with SVM and Random Forests," 2019 International Conference on Software, Telecommunications and Computer Networks (SoftCOM), Split, Croatia, 2019, pp. 1-6, doi: 10.23919/SOFTCOM.2019.8903672.
[15] Simon Duque Anton, Suneetha Kanoor, Daniel Fraunholz, and Hans Dieter Schotten. 2018. Evaluation of Machine Learning-based Anomaly Detection Algorithms on an Industrial Modbus/TCP Data Set. In Proceedings of the 13th International Conference on Availability, Reliability and Security (ARES '18). Association for Computing Machinery, New York, NY, USA, Article 41, 1–9. https://doi.org/10.1145/3230833.3232818.
[16] C. Ioannou and V. Vassiliou, "Classifying Security Attacks in IoT Networks Using Supervised Learning," 2019 15th International Conference on Distributed Computing in Sensor Systems (DCOSS), Santorini, Greece, 2019, pp. 652-658, doi: 10.1109/DCOSS.2019.00118.
[17] K. S. Sahoo et al., "An Evolutionary SVM Model for DDOS Attack Detection in Software Defined Networks," in IEEE Access, vol. 8, pp. 132502-132513, 2020, doi: 10.1109/ACCESS.2020.3009733.
[18] Mittal, M.; de Prado, R.P.; Kawai, Y.; Nakajima, S.; Muñoz-Expósito, J.E. Machine Learning Techniques for Energy Efficiency and Anomaly Detection in Hybrid Wireless Sensor Networks. Energies 2021, 14, 3125. https://doi.org/10.3390/en14113125.
[19] R. Javed, S. u. Rehman, M. U. Khan, M. Alazab and T. R. G, "CANintelliIDS: Detecting In-Vehicle Intrusion Attacks on a Controller Area Network Using CNN and Attention-Based GRU," in IEEE Transactions on Network Science and Engineering, vol. 8, no. 2, pp. 1456-1466, 1 April-June 2021, doi: 10.1109/TNSE.2021.3059881.
[20] Zhou, A.; Li, Z.; Shen, Y. Anomaly Detection of CAN Bus Messages Using a Deep Neural Network for Autonomous Vehicles. Appl. Sci. 2019, 9, 3174. https://doi.org/10.3390/app9153174.
[21] Mahmoud Said Elsayed, Nhien-An Le-Khac, Soumyabrata Dev, and Anca Delia Jurcut. 2020. Network Anomaly Detection Using LSTM Based Autoencoder. In Proceedings of the 16th ACM Symposium on QoS and Security for Wireless and Mobile Networks (Q2SWinet '20). Association for Computing Machinery, New York, NY, USA, 37–45. https://doi.org/10.1145/3416013.3426457.

[22] Z. Chen, C. K. Yeo, B. S. Lee and C. T. Lau, "Autoencoder-based network anomaly detection," 2018 Wireless Telecommunications Symposium (WTS), Phoenix, AZ, USA, 2018, pp. 1-5, doi: 10.1109/WTS.2018.8363930.
[23] S. Afroz, S. M. Ariful Islam, S. Nawer Rafa and M. Islam, "A Two Layer Machine Learning System for Intrusion Detection Based on Random Forest and Support Vector Machine," 2020 IEEE International Women in Engineering (WIE) Conference on Electrical and Computer Engineering (WIECON-ECE), Bhubaneswar, India, 2020, pp. 300-303, doi: 10.1109/WIECON-ECE52138.2020.9397945.
[24] Malaiya, Ritesh K., et al. "An empirical evaluation of deep learning for network anomaly detection." IEEE Access 7 (2019): 140806-140817.
[25] Alshammari, A., Zohdy, M.A., Debnath, D. and Corser, G. (2018) Classification Approach for Intrusion Detection in Vehicle Systems. Wireless Engineering and Technology, 9, 79-94. https://doi.org/10.4236/wet.2018.94007.
[26] Khan, J.; Lim, D.-W.; Kim, Y.-S. Intrusion Detection System CAN-Bus In-Vehicle Networks Based on the Statistical Characteristics of Attacks. Sensors 2023, 23, 3554. https://doi.org/10.3390/s23073554.
[27] He, Qiyi. (2021). A machine learning-based anomaly detection framework for connected and autonomous vehicles cyber security.
[28] U. Dincalp, M. S. Güzel, O. Sevine, E. Bostanci and I. Askerzade, "Anomaly Based Distributed Denial of Service Attack Detection and Prevention with Machine Learning," 2018 2nd International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT), Ankara, Turkey, 2018, pp. 1-4, doi: 10.1109/ISMSIT.2018.8567252.
[29] Kwak, B. I., Han, M. L., & Kim, H. K. (2021). Cosine similarity based anomaly detection methodology for the CAN bus. Expert Systems with Applications, 166, 114066.
[30] M. Marchetti and D. Stabili, "Anomaly detection of CAN bus messages through analysis of ID sequences," 2017 IEEE Intelligent Vehicles Symposium (IV), Los Angeles, CA, USA, 2017, pp. 1577-1583, doi: 10.1109/IVS.2017.7995934.
[31] Tanksale, "Design of Anomaly Detection Functions for Controller Area Networks," in IEEE Open Journal of Intelligent Transportation Systems, vol. 2, pp. 312-321, 2021, doi: 10.1109/OJITS.2021.3104495.
[32] S. Boumiza and R. Braham, "An Anomaly Detector for CAN Bus Networks in Autonomous Cars based on Neural Networks," 2019 International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), Barcelona, Spain, 2019, pp. 1-6, doi: 10.1109/WiMOB.2019.8923315.
[33] Mee Lan Han, Byung Il Kwak, Huy Kang Kim, Anomaly intrusion detection method for vehicular networks based on survival analysis, Vehicular Communications, Volume 14, 2018, Pages 52-63, ISSN 2214-2096, https://doi.org/10.1016/j.vehcom.2018.09.004.
[34] Taylor, S. Leblanc and N. Japkowicz, "Anomaly Detection in Automobile Control Network Data with Long Short-Term Memory Networks," 2016 IEEE International Conference on Data Science and Advanced Analytics (DSAA), Montreal, QC, Canada, 2016, pp. 130-139, doi: 10.1109/DSAA.2016.20.
[35] V. Tanksale, "Anomaly Detection for Controller Area Networks Using Long Short-Term Memory," in IEEE Open Journal of Intelligent Transportation Systems, vol. 1, pp. 253-265, 2020, doi: 10.1109/OJITS.2020.3043066.
[36] Hongmao Qin, Mengru Yan, Haojie Ji, Application of Controller Area Network (CAN) bus anomaly detection based on time series prediction, Vehicular Communications, Volume 27, 2021, 100291, ISSN 2214-2096, https://doi.org/10.1016/j.vehcom.2020.100291.
[37] J. Ning, J. Wang, J. Liu and N. Kato, "Attacker Identification and Intrusion Detection for In-Vehicle Networks," in IEEE Communications Letters, vol. 23, no. 11, pp. 1927-1930, Nov. 2019, doi: 10.1109/LCOMM.2019.2937097.
[38] Y. Linghu, M. Xu, X. Li and H. Qian, "Weighted Local Outlier Factor for Detecting Anomaly on In-Vehicle Network," 2020 16th International Conference on Mobility, Sensing and Networking (MSN), Tokyo, Japan, 2020, pp. 479-487, doi: 10.1109/MSN50589.2020.00082.
[39] van Wyk, Y. Wang, A. Khojandi and N. Masoud, "Real-Time Sensor Anomaly Detection and Identification in Automated Vehicles," in IEEE Transactions on Intelligent Transportation Systems, vol. 21, no. 3, pp. 1264-1276, March 2020, doi: 10.1109/TITS.2019.2906038.
[40] 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, doi: 10.1109/PST.2017.00017.
[41] F. Amato, L. Coppolino, F. Mercaldo, F. Moscato, R. Nardone and A. Santone, "CAN-Bus Attack Detection With Deep Learning," in IEEE Transactions on Intelligent Transportation Systems, vol. 22, no. 8, pp. 5081-5090, Aug. 2021, doi: 10.1109/TITS.2020.3046974.
[42] Subir Halder, Mauro Conti, and Sajal K. Das. 2020. COIDS: A Clock Offset Based Intrusion Detection System for Controller Area Networks. In Proceedings of the 21st International Conference on Distributed Computing and Networking (ICDCN '20). Association for Computing Machinery, New York, NY, USA, Article 22, 1–10. https://doi.org/10.1145/3369740.3369787
[43] T. Moulahi, S. Zidi, A. Alabdulatif and M. Atiquzzaman, "Comparative Performance Evaluation of Intrusion Detection Based on Machine Learning in In-Vehicle Controller Area Network Bus," in IEEE Access, vol. 9, pp. 99595-99605, 2021, doi: 10.1109/ACCESS.2021.3095962.
[44] S. Katragadda, P. J. Darby, A. Roche and R. Gottumukkala, "Detecting Low-Rate Replay-Based Injection Attacks on In-Vehicle Networks," in IEEE Access, vol. 8, pp. 54979-54993, 2020, doi: 10.1109/ACCESS.2020.2980523.
[45] E. Seo, H. M. Song and H. K. Kim, "GIDS: GAN based Intrusion Detection System for In-Vehicle Network," 2018 16th Annual Conference on Privacy, Security and Trust (PST), Belfast, Ireland, 2018, pp. 1-6, doi: 10.1109/PST.2018.8514157.
[46] Lokman, SF., Othman, A.T. & Abu-Bakar, MH. Intrusion detection system for automotive Controller Area Network (CAN) bus system: a review. J Wireless Com Network 2019, 184 (2019). https://doi.org/10.1186/s13638-019-1484-3.
[47] Fusheng Jin, Mengnan Chen, Weiwei Zhang, Ye Yuan, Shuliang Wang, Intrusion detection on internet of vehicles via combining log-ratio oversampling, outlier detection and metric learning, Information Sciences, Volume 579, 2021, Pages 814-831, ISSN 0020-0255, https://doi.org/10.1016/j.ins.2021.08.010.
[48] S. Purohit and M. Govindarasu, "ML-based Anomaly Detection for Intra-Vehicular CAN-bus Networks," 2022 IEEE International Conference on Cyber Security and Resilience (CSR), Rhodes, Greece, 2022, pp. 233-238, doi: 10.1109/CSR54599.2022.9850292.
[49] . Avatefipour et al., "An Intelligent Secured Framework for Cyberattack Detection in Electric Vehicles' CAN Bus Using Machine Learning," in IEEE Access, vol. 7, pp. 127580-127592, 2019, doi: 10.1109/ACCESS.2019.2937576.
[50] Bi, Z., Xu, G., Xu, G., Tian, M., Jiang, R., & Zhang, S. (2022). Intrusion Detection Method for In-Vehicle CAN Bus Based on Message and Time Transfer Matrix. Security and Communication Networks, 2022(1), 2554280. https://doi.org/10.1155/2022/2554280.
[51] POLCÁK, Libor; FRANKOVÁ, Barbora. Clock-Skew-Based Computer Identification: Traps and Pitfalls. J. Univers. Comput. Sci., 2015, 21.9: 1210-1233.
[52] S. U. Sagong, X. Ying, A. Clark, L. Bushnell and R. Poovendran, "Cloaking the Clock: Emulating Clock Skew in Controller Area Networks," 2018 ACM/IEEE 9th International Conference on Cyber-Physical Systems (ICCPS), Porto, Portugal, 2018, pp. 32-42, doi: 10.1109/ICCPS.2018.00012.
[53] D. Stabili and M. Marchetti, "Detection of Missing CAN Messages through Inter-Arrival Time Analysis," 2019 IEEE 90th Vehicular Technology Conference (VTC2019-Fall), Honolulu, HI, USA, 2019, pp. 1-7, doi: 10.1109/VTCFall.2019.8891068.
[54] X. Ying, S. U. Sagong, A. Clark, L. Bushnell and R. Poovendran, "Shape of the Cloak: Formal Analysis of Clock Skew-Based Intrusion Detection System in Controller Area Networks," in IEEE Transactions on Information Forensics and Security, vol. 14, no. 9, pp. 2300-2314, Sept. 2019, doi: 10.1109/TIFS.2019.2895957.
[55] S. Lee, H. J. Jo, A. Cho, D. H. Lee and W. Choi, "TTIDS: Transmission-Resuming Time-Based Intrusion Detection System for Controller Area Network (CAN)," in IEEE Access, vol. 10, pp. 52139-52153, 2022, doi: 10.1109/ACCESS.2022.3174356.
[56] Kyong-Tak Cho and Kang G. Shin. 2016. Fingerprinting electronic control units for vehicle intrusion detection. In Proceedings of the 25th USENIX Conference on Security Symposium (SEC'16). USENIX Association, USA, 911–927.
[57] Sunny, S. Sankaran and V. Saraswat, "A Hybrid Approach for Fast Anomaly Detection in Controller Area Networks," 2020 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), New Delhi, India, 2020, pp. 1-6, doi: 10.1109/ANTS50601.2020.9342791.
[58] Zhou, P. Joshi, H. Zeng, and R. Li, "Btmonitor: Bit-time-based intrusion detection and attacker identification in controller area network," ACM Transactions on Embedded Computing Systems (TECS), vol. 18, no. 6, pp. 1–23, 2019.

[59] Zhou, G. Xie, S. Yu and R. Li, "Clock-Based Sender Identification and Attack Detection for Automotive CAN Network," in IEEE Access, vol. 9, pp. 2665-2679, 2021, doi: 10.1109/ACCESS.2020.3046862.

[60] Tomlinson, J. Bryans, S. A. Shaikh and H. K. Kalutarage, "Detection of Automotive CAN Cyber-Attacks by Identifying Packet Timing Anomalies in Time Windows," 2018 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W), Luxembourg, Luxembourg, 2018, pp. 231-238, doi: 10.1109/DSN-W.2018.00069.

[61] H. Ji, Y. Wang, H. Qin, X. Wu and G. Yu, "Investigating the Effects of Attack Detection for In-Vehicle Networks Based on Clock Drift of ECUs," in IEEE Access, vol. 6, pp. 49375-49384, 2018, doi: 10.1109/ACCESS.2018.2841884.

[62] RUTH, R., BARTLETT, W., AND DAILY, J. Accuracy of event data in the 2010 and 2011 Toyota camry during steady state and braking conditions. In SAE International Journal on Passenger Cars (2012).

[63] DAILY, J. Analysis of critical speed yaw scuffs using spiral curves. In SAE Technical Paper 2012-01-0606 (2012).

[64] D. Stabili and M. Marchetti. (2019) VTC2019Fall Dataset. [Online]. Available: https://weblab:ing:unimore:it/people/stabili/resources.

[65] H. Lee, S. H. Jeong and H. K. Kim. 2018. CAN Dataset for intrusion detection (OTIDS). [Online]: http://ocslab.hksecurity.net/Dataset/CAN-intrusion-dataset. (2018). Accessed on October 15, 2018.

[66] Mattia Zago et al. ReCAN Data - Reverse engineering of Controller Area Networks", Mendeley Data, v2. 2020. URL:http://dx.doi.org/10.17632/76knkx3fzv.2#folder3d76230-b403-4d8 -972e-9fcdfd3cd30c.

[67] Han ML, Kwak BI, Kim HK. Anomaly intrusion detection method for vehicular networks based on survival analysis. Vehicular Comms. 2018;doi:10.1016/j.vehcom.2018.09.004.

[68] Seo E, Song HM, Kim HK. GIDS: GAN based Intrusion Detection System for In-Vehicle Network. In: PST; 2018.

[69] Song HM, Woo J, Kim HK. In-vehicle network intrusion detection using deep convolutional neural network. Vehicular Communications. 2020;doi:10.1016/j.vehcom.2019.100198.

[70] Dupont G, Lekidis A, Den Hartog J, Etalle S. Automotive Controller Area Network (CAN) Bus Intrusion Dataset v2; 2019.

[71] Verma, M.E., Iannacone, M.D., Bridges, R.A., Hollifield, S.C., Moriano, P., Kay, B., & Combs, F.L. (2020). A comprehensive guide to CAN IDS data and introduction of the ROAD dataset. PLOS ONE, 19.

[72] S. Jin, J. -G. Chung and Y. Xu, "Signature-Based Intrusion Detection System (IDS) for In-Vehicle CAN Bus Network," 2021 IEEE International Symposium on Circuits and Systems (ISCAS), Daegu, Korea, 2021, pp. 1-5, doi: 10.1109/ISCAS51556.2021.9401087.

[73] Tayyab, M., Hafeez, A., & Malik, H. (2018, August). Spoofing attack on clock-based intrusion detection system in controller area networks. In NDIA Ground Vehicle Systems Engineering and Technology Symposium, Novi, Michigan (pp. 1-13).

[74] Maliha, Maisha, and Shameek Bhattacharjee. "A Unified Time Series Analytics based Intrusion Detection Framework for CAN BUS Attacks." Proceedings of the Fourteenth ACM Conference on Data and Application Security and Privacy. 2024.

[75] Lokman, SF., Othman, A.T. & Abu-Bakar, MH. Intrusion detection system for automotive Controller Area Network (CAN) bus system: a review. J Wireless Com Network 2019, 184 (2019). https://doi.org/10.1186/s13638-019-1484-3.