An example of Hybrid IDS based on new ML method to improve the precision and effciency in recognition of attacks on connected vehicles infrastructure

Autors: Maiorana Angela[1], Luigi Passariello[1], Stefano Iannello[1], Giuseppe Passariello[2], Michele Passariello[2],

1. CRSLAGHI- Centro Ricerche e Studi dei laghi, Milan
2. Ma.Pa.COM Advanced Technologies, Department of Research & Development, Milan (Italy)

Keywords: IDS (Intrution Detection System), Deep Learning, Expert systems, Cybersecurity

Abstract

The experimentation involved the application of Deel Learning methods for the early identification of cyber attacks. The scope of application is that of the automotive sector, in which monitoring and information exchange networks are relevant for the safety of drivers and travellers. However, the application of the tested methods can be used in general for all monitoring networks. The results obtained using an innovative BARC algorithm (Best Algorith for Right Class), which works as a combination of other DL algorithms, have allowed a significant improvement in the early recognition of cyber attacks.

INTRODUCTION

One of the most pressing issues at the center of the current digital transition scenario in the automotive sector is cybersecurity in connected cars. The advanced digital technologies installed in the latest generation cars make driving easier and easily satisfy the needs of motorists, be they finding the best route or introducing autonomous driving. [25] illustrates how the growth of the Italian connected car market increased by 8% compared to 2020. In 2021 almost one in two cars in circulation was a connected car. Added to this is also the publication of the European legislation of 19 September 2019, which made ADAS (Advanced Driver Assistance Systems) technology mandatory in all cars registered starting from 2022. At a global level, an analysis by Juniper Research estimates that, by 2027, 97% of cars in circulation will be connected. Following this trend, the road towards a future totally characterized by connected cars seems clear. But how can we work at a cybersecurity level in connected cars to protect driving safety and passenger privacy? The risk of cyber attacks and data theft through the connection systems of connected cars, as with any other digital technology, is in fact always lurking. Connected cars, like PCs and smartphones, can suffer a hacker attack through various vulnerable points. This is at the expense of the safety and privacy of passengers, because hackers could intercept phone calls, steal data and alter the autonomous driving mode. The systems that can be hacked are mainly the on-board system, the infotainment (a display installed on board that allows you to receive information on traffic, the climate, listen to music and make calls) or the connectivity system. To avoid the danger of cyber attacks, malware or ransomware and any other vulnerabilities, the automotive industry is introducing high security measures at every level of the supply chain:

- Security measures are implemented within the production departments in the IT systems, in the connected machinery (Industrial Internet of Things) and in the related IT networks;

- In cloud infrastructures and applications, ADAS (driving assistance), infotainment, remote diagnostics, predictive maintenance, navigation and similar systems are protected;
- We intervene in the internal structure of the car by protecting the Central gateway (the system that transfers data inside the car), the Powertrain (i.e. the propulsion unit), and the Chassis control (the electric suspension regulator);
- In external interfaces, we work to constantly protect Wi-Fi, Bluetooth, USB, GPS networks.

Regulations to safeguard cybersecurity in connected cars

To address the problem of hacker attacks, automakers are investing in advanced security systems at every level of the supply chain.

In addition to providing multi-factor authentication measures and increasingly effective attack detection systems, manufacturers observe three main regulations to guarantee maximum cybersecurity on board:

- **IEC 62443**, which regulates the safety of production sites in terms of cybersecurity for OT (Operational Technology), automation and control systems;
- **ISO/SAE 21434**, which aims to ensure that manufacturers are able to identify, analyze and manage the risks of cyber attacks throughout the entire life cycle of the vehicle;
- **UNECE R155** and **UNECE 156**, which define specific cybersecurity obligations for all vehicles, establishing the implementation of IT security management systems and software updates. These compliances will apply from July 2024 to all new vehicles.

The test to guarantee safety in connected cars

Before being placed on the market, connected cars must also pass the penetration test required by UNECE R155 and UNECE 156. The test verifies the effective resistance to cyber attacks and the general level of cyber security of the vehicle through simulations of hacker attacks. The elements taken into consideration are wireless and mobile networks, the communication system of the car with other cars (V2V) and of the car with the infrastructure (V2I).

State of art

İsa Avcı and Murat Koca have explored performance of four ML techniques, the Random Forest (RF), K-Nearest Neighbors (KNN), Support Vector Machine (SVM) and the Decision Tree (DT) systems for intrusion detection system in automotive, Canzone et al. [16] proposed a deep convolutional neural network model framework for in-vehicle intrusion detection. This model shows high performance in Car-Hacking. Zhao et al. [17] proposed an IDS framework for IoT systems based on deep neural network models. Yang et al. [18] proposed a stacking ensemble framework for network intrusion detection in IoV systems using tree-based ML models. The model shows high accuracy on CAN intrusion and CICIDS2017 dataset. Elmasry et al. [19] proposed an ensemble model for network intrusion detection using three deep learning models: Deep Neural Networks (DNN), Long Short Term Memory (LSTM), and Deep Belief Networks (DBN). Chen et al. [20] proposed a new IDS framework called All Predict Wisest Decides (APWD), to detect intrusions and make decisions based on the wisest model for each class but with performance lower than 80%.

Although many of the related works achieve high performance in intrusion detection tasks of IoV systems, there is still much room to improve the state-of-the-art performance. IDS frameworks can be improved

and enhanced by making more use of advanced ML algorithms and ensemble strategies. The proposed solution aims to exploit both leader class and prediction based on trust strategies to construct ensemble IDS. The use of three advanced gradient enhancement algorithms also improves the effectiveness of intrusion detection.

The attachment elements of a connected vehicle

In the automotive sector where the technological landscape is constantly evolving, the integration between artificial intelligence (AI) and cybersecurity represents a significant evolution of innovation that can allow the safety level of connected vehicles to be raised. In reality, the adoption of AI-based tools and techniques in cyber security is no longer just an optional strategy, but a necessity to counter the increase in the sophistication of cyber attacks.

However, the growing connectivity of the Internet of Vehicles (IoV) increases vulnerability to network attacks. To protect IoV systems against cyber threats, Intrusion Detection Systems (IDS) have been developed that can identify malicious cyber attacks, using Machine Learning (ML) approaches. The project activity focused in particular on the use of Deep Learning algorithms for the early and adaptive recognition of alarms and their management according to a BARC (Best Algorith for Right Class) approach, i.e. to use for the various types of attacks the most performing recognition algorithm.

Below, an overview of the application potential of Artificial Intelligence (AI) in the field of cyber security and helping to protect the digital frontier.

1. **Threat detection and prevention** – AI-based systems can analyze large amounts of data, identify patterns and detect anomalies in real time. Additionally, AI, leveraging Machine Learning (ML) algorithms, can detect known threats and identify new and sophisticated attack vectors that traditional rule-based systems may miss. AI can also proactively identify vulnerabilities in networks and systems, allowing organizations to patch them before they can be exploited.
2. **Behavioral Analysis** – AI can monitor and analyze user behavior, network traffic, and system logs to identify unusual patterns or suspicious activity. AI algorithms, by establishing baselines and understanding normal behavior, can identify deviations and send alerts when potential threats are detected. This helps detect threats on the internal network, malware infections or unauthorized access attempts.
3. **Automated response and mitigation** – AI can enable automated responses to cyber security incidents, reducing response times and minimizing the impact of attacks. AI systems, for example, can autonomously block suspicious IP addresses, quarantine infected devices or initiate incident response procedures based on predefined rules and policies. This allows organizations to respond quickly and effectively to mitigate threats.
4. **Threat intelligence and analytics** – AI can help collect, analyze and correlate large volumes of threat intelligence data from various sources. Additionally, AI algorithms can identify emerging threats, analyze attack patterns, and provide actionable insights to security teams. This helps in proactively identifying threats, assessing vulnerabilities and developing robust defense strategies.
5. **Adversarial machine learning** – Adversarial machine learning involves using AI to identify and defend against attacks that target the same machine learning models. In fact, adversaries can attempt to manipulate or evade detection by exploiting vulnerabilities in AI algorithms. AI techniques, such as adversarial training and anomaly detection, can help detect and mitigate these attacks, ensuring the integrity and reliability of AI-based security systems.

6. **Improved authentication and access control** – AI can strengthen authentication mechanisms using biometrics, facial recognition, voice recognition and behavioral analytics. These techniques help verify user identities more accurately, reducing the risk of unauthorized access or account compromise. Additionally, AI-based access control systems can also adapt and learn from user behaviors to detect suspicious activity and prevent unauthorized access attempts.
7. **Security automation and orchestration** – AI can automate routine security tasks and workflows, allowing human analysts to focus on more complex and strategic tasks. AI-powered security orchestration platforms can integrate various security tools, streamline incident response processes, and provide centralized visibility into security operations. This improves efficiency, reduces response times and improves the overall cybersecurity posture**.**

Finally, it should be noted that the future of the automotive sector foresees a gradual replacement of conventional vehicles [1] with autonomous vehicles (AV) and connected vehicles (CV) and the development of Internet of Vehicles (IoV) technologies, i.e. car networks that exchange information in cooperative manner. To protect IoV systems and connected cars in general against cyber threats, Intrusion Detection Systems (IDS) have been developed that can identify malicious cyber attacks, using Machine Learning (ML) approaches. However, there is room for improvement both in the precision (i.e. minimization of false rejections and false acceptances) with which attacks are detected and recognized which obviously allows for earlier defense interventions such as the inhibition of some addresses used by attackers and the isolation of components that may have been infected and therefore no longer be reliable.
The results of this research were obtained in a project financed by the Campania Region, called Borgo 4.0, as part of the P-Mobility sub-project aimed at creating a support infrastructure for the various platforms for monitoring and processing data relating to safety and to autonomous driving.

The attachment elements of a connected vehicle

The attack targets of a connected vehicle are as follows:

- Component of the external network or external systems that communicate with the vehicle (Mobile, Wireless)
- Internal vehicle network (CAN BUS Attack) through direct access or using the wireless connection

In the following figure we highlight the access roads and objectives of a generic attacker and the defense role played by the Intrusion Detection System (IDS).

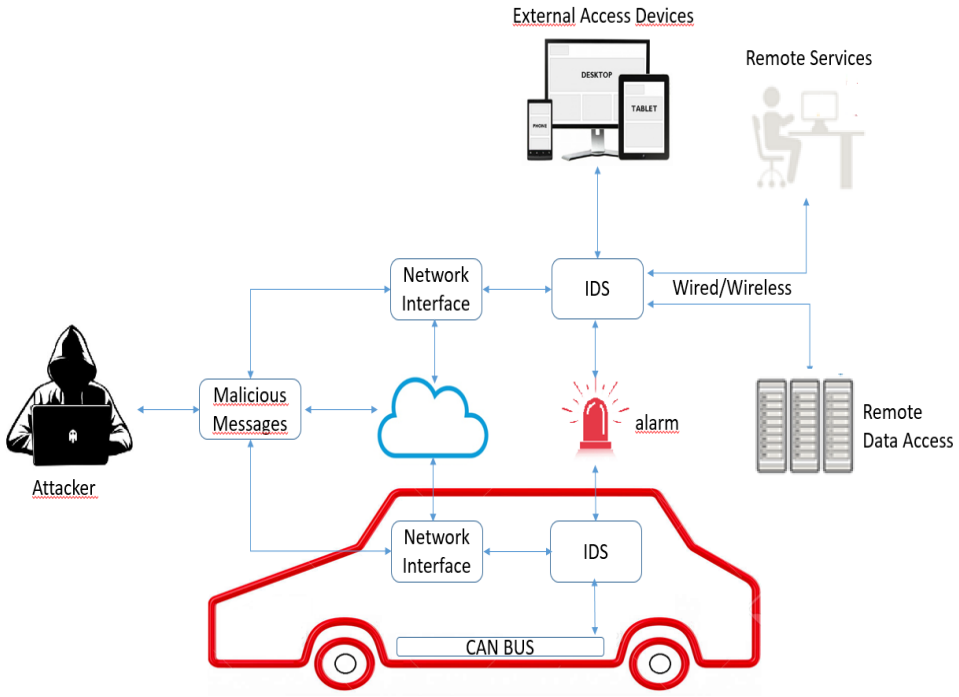

Figure 1 - Vehicle architecture protected by IDS.

In the figure we can distinguish two network interfaces, one towards the network external to the vehicle and one towards the internal network.

- In Internal Vehicle Networks (IVNs), the Controller Area Network (CAN) bus is the main infrastructure enabling communication between electronic control units (ECUs) to implement various functionalities [2].
- External vehicular networks, on the other hand, use Vehicle-To-Everything (V2X) technology to enable the connection between smart cars and other IoV entities, such as road units, infrastructure and smart devices [3].

MATERIALS AND MODELS

To accurately detect various types of attacks in IoV networks, we propose a hybrid and adaptive IDS. Through the analysis of network traffic data, ML approaches can be employed to build classifier-based IDSs that can distinguish between benign network events and various cyber attacks [8] [9]. To apply ML models to IDS systems, it is useful to observe how the prediction performance of different ML models varies significantly for different types of cyber attacks.

Models tested

We start by determining the best performing ML model among an advanced number of ML algorithms;

- KNN [28]

- RF [28]
- LSTM-AE [26, 24]
- DCNN [27]
- DBN [19]
- Stacking [18]
- LightGBM [11]
- XGBoost [10]
- CatBoost [12]

The last three algorithms, XGBoost, LightGBM, and CatBoost, have some advantages over the others [10] - [12]:

1. These three ML models are all robust ensemble models that have been highly successful in a variety of data analytics applications [22].
2. These three ML models can automatically generate feature importance scores and select features during their training process, which saves time and resources by avoiding the need to design additional features.
3. These three ML models are fast models with relatively low computational complexity. In addition, they all support parallelization and graphics processing unit (GPU), which can further improve the model learning speed.
4. These three ML models include randomness in their model building processes, allowing people to develop a robust ensemble model with high diversity and generalizability.

Datasets

To carry out training and testing, two public datasets are used to test the safety of connected cars and in general in the context of IoVs.

1. Car-Hacking

ATTACK TYPE	# OF MESSAGES	# OF NORMAL MESSAGES	# OF INJECTED MESSAGES
DoS Attack	3,665,771	3,078,250	587,521
Fuzzy Attack	3,838,860	3,347,013	491,847
Spoofing the drive gear	4,443,142	3,845,890	597,252
Spoofing the RPM gauze	4,621,702	3,966,805	654,897
GIDS: Attack-free	988,987	988,872	-

2. CICIDS2017

CICIDS2017 dataset contains benign and the most up-to-date common attacks, which resembles the true real-world data (PCAPs). It also includes the results of the network traffic analysis using CICFlowMeter with labeled flows based on the time stamp, source, and destination IPs, source and destination ports, protocols and attack (CSV files). Also available is the extracted features definition.

Generating realistic background traffic was our top priority in building this dataset. We have used our proposed B-Profile system (Sharafaldin, et al. 2016) to profile the abstract behavior of human interactions and generates naturalistic benign background traffic. For this dataset, we built the abstract behaviour of 25 users based on the HTTP, HTTPS, FTP, SSH, and email protocols.

The data capturing period started at 9 a.m., Monday, July 3, 2017 and ended at 5 p.m. on Friday July 7, 2017, for a total of 5 days. Monday is the normal day and only includes the benign traffic. The implemented attacks include

- Brute Force FTP,
- Brute Force SSH,
- DoS,
- Heartbleed,
- Web Attack,
- Infiltration,
- Botnet
- DDoS.

They have been executed both morning and afternoon on Tuesday, Wednesday, Thursday and Friday.

DISDCUSSION AND RESULTS

Methodology

It may happen that an algorithm recognizes the attack elements of a given class compared to other algorithms. For example, an algorithm can better recognize DOS attacks and fewer attacks. For this reason we propose an innovative methodology to improve the reliability of threat identification results based on the analysis and interpretation of the results of three attack training and recognition models.

The aim of this work is to develop an IDS Framework capable of effectively detecting various types of attacks on both IVNs and external vehicular networks.

Through the training phase, The algorithm aims to obtain adaptive models optimized for all attack classes through the following steps:

1. Train all considered ML models using the datasets.
2. Evaluate the performance of each ML model for each class (normal or attack type) using cross-validation and F1 scores. F1 scores are chosen because it is a comprehensive performance metric and works well with imbalanced datasets.
3. Determine the best performing model for each class in terms of execution time and maximum F1 score. This model is used as the reference model for that class. If multiple ML models achieve higher F1 scores, the ML model can be chosen as the fastest model among them.

Best result is achieved by best model for that type of attack. The following figure shows the functional scheme of the proposed algorithm:

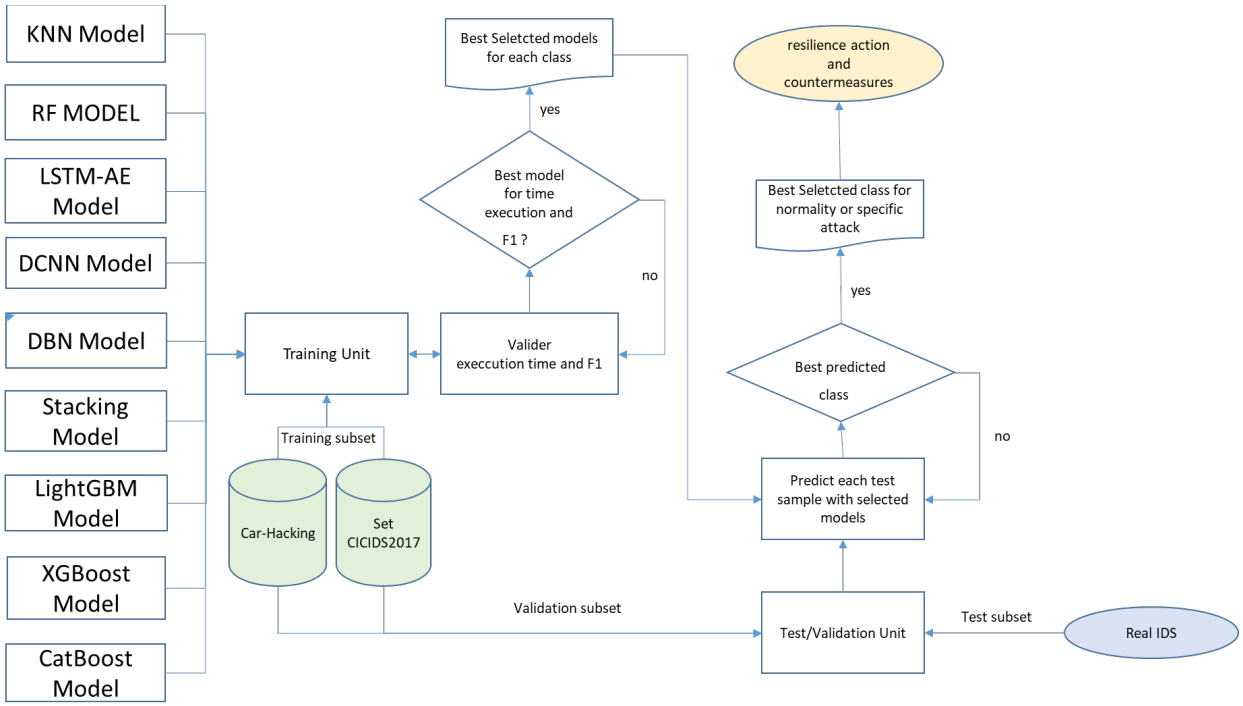

Figure 2 – The new algorithm proposed for hybrid and adaptive IDS.

Performance Evaluation

To develop the proposed IDS, models were implemented using Python libraries. The experiments were conducted on a Dell Precision 3630 Computer with i9-12900HK processor and 32 GB of memory, representing an IoV server machine.

The performance of the system is evaluated using the two public datasets, previously introduced, with data on the main security attacks of the public reference IoV network,

- Car-Hacking[13] e
- CICIDS2017 [14]

which represent the IVN and external network data respectively.

The Car-Hacking dataset [13] is created by transmitting CAN messages to a real CAN bus vehicle. It has nine characteristics (i.e., CAN ID and eight bits of the CAN message data field) and four attack types (i.e., DoS, fuzzy, gear spoofing, and revolutions per minute (RPM) spoofing).

The CICIDS2017 dataset [14] is a state-of-the-art general cybersecurity dataset, including the most up-to-date attack types (e.g., DoS, sniffing, brute force, web attacks, botnets, and infiltration attacks).

To evaluate the proposed optimization model, the datasets were divided into two subsets containing 80% and 20% of the samples respectively. They are used for training and validation test. Network traffic data

is often highly imbalanced and contains only a small percentage of attack samples. For training and testing purposes, four performance measures, including accuracy, precision, recall, and F1 scores, are used to evaluate model performance [3]. The execution time in terms of training tests of the model are used to evaluate the model from the point of view of efficiency. The experimental results of the evaluation of the ML models applied to obtain evaluations useful for the realization of the evolved model proposed with this activity, using the Car-Hacking and CICIDS2017 datasets, are reported in Tables I, II and III.

Table I- EVALUATION OF MODEL PERFORMANCE ON THE **CAR-HACKING DATASET** (AVERAGE VALUES OVER ALL CLASSES)

Model	Accuracy	Precision	Recall	F1 (%)	Time for training set	Time for Validation set	Time for single attack test
KNN	97.5	96.3	98.4	94.1	1297.7	29,655	O,071
SVM	96.5	95.8	98.41	93.5	1388.2	222,112	O,078
LSTM-AE	98.78	98.31	98.71	95.1	682.44	95,5416	O,0745
DCNN	97.5	88.45	98.34	96.5	723.645	108,5468	O,0715
RF	98.22	98.99	98.87	98.30	346.1	51,915	O,0445
DBN	99.20	98.32	98.52	97.32	788.32	126,1312	O,0622
Stacking	99.80	99.75	99.89	99.70	278.8	44,608	O,0754
LightGBM	99.9997	99.9997	99.9997	99.9997	62.5	1,875	O,0645
XGBoost	99.9994	99.9994	99.9994	99,99896	66.6	6,524	O,0745
CatBoost	99.9994	99.9994	99.9994	99,99792	95.8	14,37	O,0768
Hybrid model proposed	99.9997	99.9997	99.9997	99,9997	130.3	29,808	O,0845

Tabella II - PERFORMANCE EVALUATION OF MODELS ON THE **CICIDS2017 DATASET** (AVERAGE VALUES OVER ALL CLASSES)

Model	Accuracy	Precision	Recall	F1 (%)	Time for Training set	Time for Validation set	Time for single attack Test
KNN	96.3	96.2	93.7	96.3	1558.3	O,0045	O,0045
SVM	98.5	98.8	98.41	97.5	1388.2	222,112	O,078
LSTM-AE	99.1	99.1	99.91	97.1	682.44	O,0045	O,0045
DCNN	99.22	99.38	99.33	97.18	723.645	O,0045	O,0045
RF	98.82	98.8	98.955	97.11	35.1	O,0045	O,0045

DBN	98.95	95.82	95.81	95.81	228.32	O,0045	O,0045
Stacking	98.80	98.75	98.22	97.20	278.8	O,0045	O,0045
LightGBM	99.62	99.62	99.62	97.31	14.7	O,0045	O,0045
XGBoost	99.77	99.77	99.77	97,7203	44.8	O,0045	O,0045
CatBoost	99.62	99.62	99.62	97,73629	73.9	O,0045	O,0045
Hybrid model proposed	99.813	99.814	99.913	97,60386	168.9	O,0045	O,0045

Since the values of the LightGBM, XGBoost, CatBoost models and the proposed hybrid model seem to provide better performance, let's see how they performed for each class by choosing F1 which is a complete performance metric and works well with unbalanced datasets.

Tabella III - COMPARISON OF MODEL PERFORMANCE FOR EACH CLASS IN THE TWO DATA SETS

Model	**Dataset Car-Hacking**					**Dataset CICDS2017**						
Class n°	**1**	**2**	**3**	**4**	**5**	**1**	**2**	**3**	**4**	**5**	**6**	**7**
Metric Adopted	**F1**	**F1**	**F1**	**F1**	**F1**	**F1**	**F1**	**F1**	**F1**	**F1**	**F1**	**F1**
Class Name	**Normal**	**Dod**	**Fuzzy**	**Gear Spoofing**	**RPM Spoofing**	**Normal**	**Dos**	**Sniffing**	**Brute force**	**Web Attack**	**Botnets**	**Infiltration**
LightGBM	99,9998	100	99,995	100	100	99,863	100	99,889	99,222	99,3541	100	85,714
XGBoost	99,9996	100	99,990	100	100	99,863	100	99,889	99,551	99,137	100	85,714
CatBoost	99,9996	100	99,990	100	100	99,754	99,754	99,557	99,094	99,354	100	85,714
Adaptive Model	99,9996	100	99,995	100	100	99,863	100	99,889	99,551	99,354	100	85,714

È evidente che i punteggi F1 di diversi modelli ML base variano a seconda dei diversi tipi di rilevamento degli attacchi..

Il modello di ottimizzazione proposto ottiene un punteggio F1 quasi perfetto sul set di dati Car-Hacking (99,9997%) e ha migliorato il suo punteggio F1 da 99,792% a 99,811% sul set di dati CICIDS2017. Ciò dimostra i vantaggi derivanti dall'identificazione dei modelli base con le migliori prestazioni per ciascuna classe per costruire il modello dell'insieme ottimizzato oggetto della sperimentazione.

Il modello ottimizzato proposto supera gli altri metodi di almeno lo 0,09% e miglioramenti del punteggio F1 dello **2,5480 %** sul Car-Hacking e **0,5072 %** sul set di dati CICIDS2017, rispettivamente.

Come approccio d'insieme, il modello proposto ha un tempo di esecuzione più lungo di gli altri altri modelli (LightGBM, XGBoost, CatBoost) base di potenziamento del gradiente, ma è ancora più veloce di molti altri algoritmi ML, come K-Nearest Neighbors (KNN) e Support Vector Machine (SVM).

Questo perché il modello d'insieme proposto è costruito utilizzando modelli ML di bassa complessità con esecuzione parallela e GPU di supporto. Per riassumere, il modello proposto può raggiungere i punteggi F1 più alti tra i metodi confrontati con tempo di esecuzione relativamente basso sui due set di dati di riferimento.

CONCLUSIONS

The automotive sector is organizing itself on the cybersecurity front to prevent attacks on the IT systems of connected cars. By 2027, almost all cars in circulation worldwide will be of the "connected car" type. For this reason, the defense measures that manufacturers are adopting to prevent hacker attacks must be improved. With the activities of this research we have provided a contribution to the use of new ML methods that exploit different models to calculate how each of them behaves with respect to the various attack classes analysed. It was possible to see how the algorithm which, for each type of attack class, makes differentiated use of the best performing recognition model, allows for a significant improvement in the accuracy of identification of the type of attack. Although the main metrics evaluating the identification ability of each attack class were used (Accuracy, Precision, Recall, F1), it should be noted that F1 presents better identification as it is a complete performance metric and works well with sets of unbalanced data

BIOGRAPHY

[1] H. Bangui and B. Buhnova, "Recent Advances in Machine-Learning Driven Intrusion Detection in Transportation: Survey," Procedia Comput. Sci., vol. 184, pp. 877–886, 2021.

[2] O. Y. Al-Jarrah, C. Maple, M. Dianati, D. Oxtoby, and A. Mouzakitis, "Intrusion Detection Systems for Intra-Vehicle Networks: A Review," IEEE Access, vol. 7, pp. 21266–21289, 2019.

[3] L. Yang and A. Shami, "A Transfer Learning and Optimized CNN Based Intrusion Detection System for Internet of Vehicles," in 2022 IEEE Int. Conf. Commun. (ICC), 2022, pp. 1–6.

[4] K. Kim, J. S. Kim, S. Jeong, J.-H. Park, and H. K. Kim, "Cybersecurity for autonomous vehicles: Review of attacks and defense," Comput. Secur., vol. 103, p. 102150, 2021.

[5] L. Yang, A. Moubayed, and A. Shami, "MTH-IDS: A Multitiered Hybrid Intrusion Detection System for Internet of Vehicles," IEEE, Internet Things J., vol. 9, no. 1, pp. 616–632, 2022.

[6] J. Jiang, F. Liu, W. W. Y. Ng, Q. Tang, W. Wang, and Q.-V. Pham, "Dynamic Incremental Ensemble Fuzzy Classifier for Data Streams in Green Internet of Things," IEEE Trans. Green Commun. Netw., pp. 1-14, 2022.

[7] M. Injadat, A. Moubayed, A. B. Nassif, and A. Shami, "Machine learning towards intelligent systems: applications, challenges, and opportunities," Artif. Intell. Rev., 2021.

[8] L. Yang, D. M. Manias, and A. Shami, "PWPAE: An Ensemble Framework for Concept Drift Adaptation in IoT Data Streams," in proc. 2021 IEEE Glob. Commun. Conf., pp. 1–6, 2021.

[9] L. Yang , A. Moubayed, A. Shami, P. Heidari, A. Boukhtouta, A. Larabi, R. Brunner, S. Preda, and D. Migault, "Multi-Perspective Content Delivery Networks Security Framework Using Optimized Unsupervised Anomaly Detection," IEEE Trans. Netw. Serv. Manag., vol. 19, no. 1, pp. 686-705, 2022.

[10] T. Chen and C. Guestrin, “XGBoost: A Scalable Tree Boosting System,in Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, 2016, pp. 785–794.
[11] G. Ke et al., “LightGBM: A highly efficient gradient boosting decision tree,” Adv. Neural Inf. Process. Syst., vol. 2017-December, no. Nips, pp. 3147–3155, 2017.
[12] L. Prokhorenkova, G. Gusev, A. Vorobev, A. V. Dorogush, and A. Gulin, “Catboost: Unbiased boosting with categorical features,” Adv. Neural Inf. Process. Syst., vol. 2018-December, no. Section 4, pp. 6638–6648, 2018.
[13] E. Seo, H. M. Song, and H. K. Kim, “GIDS: GAN based Intrusion Detection System for In-Vehicle Network,” 2018 16th Annu. Conf. Privacy, Secur. Trust, pp. 1–6, 2018.
[14] I. Sharafaldin, A. Habibi Lashkari, and A. A. Ghorbani, “Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization,” in Proc. Int. Conf. Inf. Syst. Secur. Privacy, 2018, pp. 108–116.
[15] M. Injadat, A. Moubayed, A. B. Nassif, and A. Shami, “Multi-Stage Optimized Machine Learning Framework for Network Intrusion Detection,” IEEE Trans. Netw. Serv. Manag., vol. 4537, no. c, pp. 1–14, 2020.
[16] H. M. Song, J. Woo, and H. K. Kim, “In-vehicle network intrusion detection using deep convolutional neural network,” Veh. Commun., vol. 21, p. 100198, 2020.
[17] R. Zhao et al., “A Novel Intrusion Detection Method Based on Lightweight Neural Network for Internet of Things,” IEEE Internet Things J., vol. 9, no. 12, pp. 9960-9972, 2022.
[18] L. Yang, A. Moubayed, I. Hamieh, and A. Shami, “Tree-Based Intelligent Intrusion Detection System in Internet of Vehicles,” in proc. 2019 IEEE Glob. Commun. Conf., pp. 1–6, 2019.
[19] W. Elmasry, A. Akbulut, and A. H. Zaim, “Evolving deep learning architectures for network intrusion detection using a double PSO metaheuristic,” Comput. Networks, vol. 168, 2020.
[20] Z. Chen, M. Simsek, B. Kantarci, and P. Djukic, “All Predict Wisest Decides: A Novel Ensemble Method to Detect Intrusive Traffic in IoT Networks,” in proc. 2021 IEEE Glob. Commun. Conf., pp. 1–6, 2021.
[21] L. Yang and A. Shami, “A Lightweight Concept Drift Detection and Adaptation Framework for IoT Data Streams,” IEEE Internet Things Mag., vol. 4, no. 2, pp. 96–101, 2021.
[22] L. Yang and A. Shami, “On hyperparameter optimization of machine learning algorithms: Theory and practice,” Neurocomputing, vol. 415, pp. 295–316, 2020.
[23] A. Alshammari, M. A. Zohdy, D. Debnath, and G. Corser, “Classification Approach for Intrusion Detection in Vehicle Systems,” Wirel. Eng. Technol., vol. 09, no. 04, pp. 79–94, 2018.
[24] J. Ashraf, A. D. Bakhshi, N. Moustafa, H. Khurshid, A. Javed, and A. Beheshti, “Novel Deep Learning-Enabled LSTM Autoencoder Architecture for Discovering Anomalous Events From Intelligent Transportation Systems,” IEEE Trans. Intell. Transp. Syst., pp. 1–12, 2020.
[25] Politecnico di Milano. Osservatorio Cresce il mercato della Connected Car in Italia: 1,92 mld €, +8% (osservatori.net)
[26] Brooke Lampe, Weizhi Meng, A survey of deep learning-based intrusion detection in automotive applications, Expert Systems with Applications, Volume 221, 2023, 119771, ISSN 0957-4174, https://doi.org/10.1016/j.eswa.2023.119771.
[27] P. Kaur, R. Sobti and A. Khamparia, "Simulation and Deep CNN based architecture for validation of Intelligent automotive functions," *2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, Bangalore, India, 2018, pp. 2344-2348, doi: 10.1109/ICACCI.2018.8554611.
[28] İsa Avcı and Murat Koca, Cybersecurity Attack Detection Model, Using, Machine Learning Techniques, Acta Polytechnica Hungarica, Vol. 20, No. 7, 2023