Detection Model for DDoS Attacks that generate Numerous False Authentications

# Abstract

Smart grid-based EV charging facilities are vulnerable to authentication-related DDoS attacks. Its service availability can be undermined under these attacks. A dataset for a Machine Learning (ML) model is required to detect DDoS attacks, but no relevant dataset exists. In this regard, Based on the data set collected from the Electric Vehicle (EV)-Distributed Denial-of-Service (DDoS) attack simulator, we propose the best feature combination for the detection of the attack by performing various Machine Learing (ML) algorithms. Our work minimizes the degree of distortion of feature information that occurs when combining features. Also, the distortion magnitude is quantified to explain how much distortion has occurred compared to an original feature. Our proposed ideas pick up the best feature combination with the consideration of a high sampling resolution, low information loss, high F1 score, and large feature size. Unlike existing DDoS datasets, the dataset used in this work is a special one that represents the characteristics of false authentications against EV charging infrastructure on the smart grid. Higher attack detection accuracy can be achieved by ML classification with other features representing system kernel status, resource consumption, and access time difference.

# Introduction

Electric Vehicles (EV) are eco-friendly products that do not emit carbon, and demand for them is explosively increasing in line with today's low-carbon policy [65]. As a result, the need for EV charging infrastructure is rapidly rising worldwide [66]. The EV authenticates itself in the smart grid and receives the required electric power [67]. The smart grid is a huge network-based infrastructure in which Information Technology (IT), Internet-of-things (IoT), and Operational Technology (OT) resources are organically combined [56]. Due to these architectural combination characteristics of the smart grid, cyber-attack threats to EV charging infrastructure are becoming more frequent and diverse [68]. Most recent security solutions for the EV charging infrastructure have met confidentiality through encryption and integrity through EV authentication and hash-based data verification [57-60]. Existing EV authentication protocols require parameters between EV, Charging Stations (CS), and Grid Server (GS) to be sequentially communicated and processed in a strict order [61-64]. This means the communicated parameters must be processed as a transaction, so other parameters can't intervene during communication. In this sense, an attacker can disrupt the authentication of other legitimate EVs with DDoS attacks that cause many authentication failures. Therefore, these attacks can undermine the service availability of the EV charging infrastructure.

To effectively fend off those attacks, it is necessary to detect them accurately and quickly block access to the charging infrastructure. A dataset for learning and testing a DDoS attack detection model should consist of data related to EV authentication in the smart grid. However, most of the existing DDoS datasets concern IT and IoT. Thus, no DDoS attack dataset exists concerning EV Authentication on the smart grid [1]. Basnet et al. [69] attempt to detect DDoS attacks on smart grid-based EV charging facilities using an Intrusion Detection System (IDS). However, DDoS attacks related to EV authentication are not covered. S Li et al. [70] proposes an IDS that detects hybrid DoS attacks targeting EV charging infrastructure. This paper uses a Machine Learning (ML) model based on Long-Short-Term Memory (LSTM)-Gated Recurrent Unit (GRU). However, their study does not provide datasets related to EV certification. Ring, M. et al. [71] review various DDoS datasets related to general networks. Another dataset on EV authentication is not included in this review. Hekmati, A. et al. [72] emulate DDoS attacks targeting IoT devices in a smart city and gather data. Since this paper collected data for IoT devices, it has nothing to do with EVs.

Since there is no DDoS dataset on EV authentication in the smart grid, we refer to a new dataset from the EV charging attack simulator [1]. This simulator virtually builds a smart grid-based EV charging facility to perform various DDoS attack scenarios that concern EV authentications. With this simulator, we can build the dataset needed for this research. This study recommends the best feature combination by testing various ML algorithms with the data. The best feature combination is selected based on high sampling resolution, low information loss, high F1 score, and large feature size. When combining features of different sizes, the data points of individual features may be distorted in the process of making them the same size. In this paper, a sampling technique to minimize this distortion has been discussed. We introduce the concepts of sampling resolution and information loss rate, which explain the distortion magnitude of the features. These concepts have been proven with statistics and experimental approaches. The existing DDoS and the new datasets proposed in this study are compared concerning the F1 score in DDoS attack detection. It is demonstrated that higher attack detection accuracy is achieved with our proposed dataset.

The structure of this paper is as follows.

* Methodology: This section describes the feature engineering process and the selection methods of the best feature combinations.
* Experiment Result: This section presents the result of the accuracy test of MLs on the different feature combinations.

# Background

# Methodology

This work presents a new model for detecting Denial-of-Service (DoS) and DDoS attacks targeting EV authentication protocols in EV charging facilities. We create a virtual EV charging simulator [1] to gather machine learning features. The simulator comprises three main parts: many EVs, several CS, and one GS, conducting DoS and DDoS attacks against legitimate EV authentication processes. Features are extracted and preprocessed through this simulator and tested on various ML models. We recommend the best feature combination and ML model that can most efficiently detect DDoS attacks in an EV charging environment.

텍스트, 스크린샷, 폰트, 인쇄이(가) 표시된 사진

자동 생성된 설명

Figure 1. Schematic view of the attack detection model

Figure 1 is a schematic view of the DDoS attack detection model in the EV-CS environment proposed in this paper. Our detection model comprises Perf STAT, Perf TOP, and Time Delta. Each of these features is further divided into sub-features. The sub-features of the Perf STAT contain information on system resources consumed for EV authentications and DDoS attacks in CS and GS. These sub-features consist of the number of executed instructions, branch instructions, and CPU cycles. The Perf TOP provides overhead information about processes in the operating system kernel of the CS and GS. This process overhead information indicates how much overhead occurred in each process based on executed instructions, branch instructions, and Central Processing Unit (CPU) cycles throughout the program.

## Feature Extraction

The Time Delta feature represents intervals between DDoS attacks or normal authentication trials from the EVs to the GS. All the features from the simulator go into the feature engineering processes [55]. The different types and sizes of the features are combined into several individual groups. The feature sizes in different groups may vary because the Performance Monitoring Unit (PMU) does not always collect the same amount of measuring and profiling data on a target program. These different feature sizes must be synchronized to the same feature size for machine learning classification. To make the features have the same size, we choose a feature down-sizing technique instead of a feature size extension method. Extending feature sizes has a problem of divergence on many samples. Downsizing a feature size causes some data points to be cut out when combining different features. Accordingly, a loss of feature information inevitably occurs due to the truncated data points. We contribute three main categories of features to develop our detection model based on the Perf STAT, Perf TOP, and Time Delta. We combine these features to get the best feature with high ML classification accuracy and a low information loss rate.

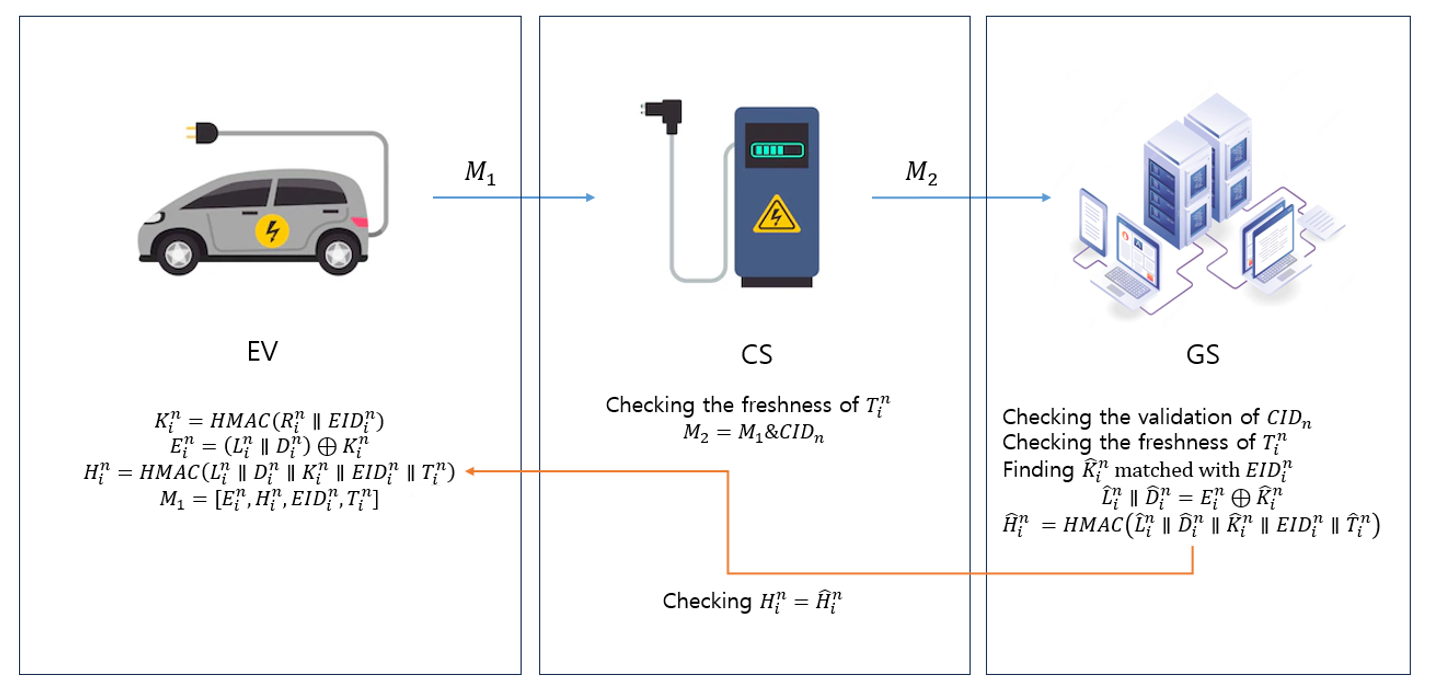


Figure 2. Schematic view of the authentication protocol on the simulator [2-11]

The authentication protocol of this simulator has been built by referring to other recent papers on EV authentication [2-11]. Figure. 2 shows the EV authentication process of the simulator used in this experiment. and are identical session keys used for message encryption and decryption, and the sizes of the keys are 256 bits. is a series of random numbers used to generate the session keys and is 128 bits in size. and are unique identification codes of EV and CS, respectively, and are 64 bits in size. and are identical to each other and indicate the location information of the EV. The sizes of and are 128 bits. and contain EV battery status information, service type, and payment information. and are identical to each other and 128 bits in size. and are timestamps, which can have different values. and have the same size of 32 bits. The EV creates through an exclusive logical OR with the value of adding and . The size of is 256 bits. Next, the EV adds , , , , and , and performs a hash operation to obtain 256-bit . The EV generates by combining , , , and , and transmits to the CS. It receives and checks whether the timestamp of the EV is valid within the time limit. The CS generates by implementing a logical product on its own with . The CS forwards this to the GS. It verifies that is matched to a valid CS, and the timestamp of that CS is fresh. The GS finds that matches and performs an exclusive OR operation with . Through this operation, and can be obtained. The GS combines , , , , and and performs a hash operation to obtain . If of the GS is equal to of the CS, the EV succeeds in the authentication. Otherwise, it fails.

### Perf STAT Features

We constructed the same normal EV charging scenario by referring to the EV charging schedule for about a year from the ACN dataset [12]. For ML features [1], system status information, such as authentication Time Deltas, system overheads, and resource consumptions, were collected through the simulator under the attacks or the normal EV charging mode. The information data is collected from the simulator using the Perf [13] with the PMU [14] inside a Central Processing Unit (CPU).

Table 1. ML feature metrics [1]

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Category  Measurement | CS or GS | | | |
| DDos Attack Mode & Normal Charging Mode | | | |
| Feature Type | | | PMU Usage Count |
| Perf TOP | Perf STAT | Time Delta |
| Instruction overheads | Yes | No | No | 3 |
| Cycle overheads | Yes | No | No |
| Branch overheads | Yes | No | No |
| Consumed instructions | No | Yes | No | 1 |
| Consumed cycles | No | Yes | No |
| Consumed branches | No | Yes | No |
| Authentication Trial | No | No | Yes | No |

Table 1 shows the criteria for collecting ML features concerning DoS and DDoS attacks on the simulator using the Perf. The Perf Top measures the system kernel overheads for instructions, cycles, and branches on the target CS and GS. Based on those criteria, the measured results are records of the Linux kernel overheads. The Perf STAT measures instructions, cycles, and branches consumed in the CS and GS Linux kernels. The Time Delta is the interval between the EVs accessing the CS and GS for normal authentication or attacks. Recent DoS and DDoS detection model studies [15-25] have applied the Time Delta as an ML feature to specialized Internet-of-Things (IoT) and general-purpose Intrusion Detection System (IDS) environments. Therefore, our research uses the Time Delta feature as a general DoS detection feature to compare with our proposed Perf TOP and Perf STAT features. Based on the metrics presented in Table 1, we collected data under various DDoS-related attack scenarios. This paper constitutes various DDoS attack scenarios against EV charging facilities.

Table 2. Attack scenarios [1]

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Major Scenario Index | Sub-Scenario Abbreviation | Random Target CS | Gaussian Analysis | Correct EV ID | Wrong CS Timestamp | Wrong EV Timestamp | Wrong EV ID |
| 1 | CID\_RCOFF\_GOFF | No | No | Yes | No | No | No |
| CID\_RCOFF\_GON | No | Yes | Yes | No | No | No |
| CID\_RCON\_GOFF | Yes | No | Yes | No | No | No |
| CID\_RCON\_GON | Yes | Yes | Yes | No | No | No |
| 2 | WCT\_RCOFF\_GOFF | No | No | No | Yes | No | No |
| WCT\_RCOFF\_GON | No | Yes | No | Yes | No | No |
| WCT\_RCON\_GOFF | Yes | No | No | Yes | No | No |
| WCT\_RCON\_GON | Yes | Yes | No | Yes | No | No |
| 3 | WET\_RCOFF\_GOFF | No | No | No | No | Yes | No |
| WET\_RCOFF\_GON | No | Yes | No | No | Yes | No |
| WET\_RCON\_GOFF | Yes | No | No | No | Yes | No |
| WET\_RCON\_GON | Yes | Yes | No | No | Yes | No |
| 4 | WID\_RCOFF\_GOFF | No | No | No | No | No | Yes |
| WID\_RCOFF\_GON | No | Yes | No | No | No | Yes |
| WID\_RCON\_GOFF | Yes | No | No | No | No | Yes |
| WID\_RCON\_GON | Yes | Yes | No | No | No | Yes |

Table 2 shows the detailed configuration of the sixteen attack scenarios. The scenarios based on DDoS attacks are derived from four major scenarios [1]. First, the attacker steals the ID of the normal EV and intentionally causes authentication failure. In Figure 2, the CS and GS take the greatest damage under this attack scenario because they must check the timestamp values, perform the XOR, and implement decryption operations. Second, he manipulates the timestamp of the CS to cause authentication failure. Since most studies [2-11] do not encrypt the timestamp value, the attacker can easily manipulate it. Second, he manipulates the timestamp of the CS to cause authentication failure. Since most studies do not encrypt the timestamp value, the attacker can easily manipulate it. Fourth, the attacker intentionally causes authentication failure by using an ID not authorized by GS. The attacker can target all CS or select some CS randomly. He can also strategically adjust the strength of the attacks to make a detection model difficult to distinguish from normal authentications. The attacker can calculate a precise DDoS attack strength to fool the detection model through a Gaussian analysis [1] of the number of normal EV authentication attempts.

The number of CS used in this study ranges from 1 to 3. Depending on the attack scenarios in Table 2, the number varies. The CPU used in the DDoS-EV Charging simulator is Intel i5 8265U and has 32 PMU counters [26]. Table 1 shows the number of PMUs required for measurement in this simulator. Since four CS and a GS are used, sixteen PMUs are required for the attack or normal modes.

### Time Delta Features

Table 3. Authentication and DDoS attack counts

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Sub-Scenario Abbreviation | Mode | Count Type | CS ID | | | GS |
| 2-39-139-28 | 2-39-131-30 | 2-39-89-25 |
| CID\_RCOFF\_GOFF | Attack | DoS | 2000 | 2000 | 2000 | 6000 |
| Authentication-1 | 324 | 245 | 213 | 782 |
| Normal | Authentication-2 | 324 | 245 | 213 | 782 |
| CID\_RCOFF\_GON | Attack | DoS | 1 | 9 | 19 | 29 |
| Authentication-1 | 324 | 245 | 213 | 782 |
| Normal | Authentication-2 | 324 | 245 | 213 | 782 |
| CID\_RCON\_GOFF | Attack | DoS | N/A | 2000 | 2000 | 4000 |
| Authentication-1 | N/A | 245 | 213 | 458 |
| Normal | Authentication-2 | N/A | 245 | 213 | 458 |
| CID\_RCON\_GON | Attack | DoS | 0 | 0 | N/A | 0 |
| Authentication-1 | 324 | 245 | N/A | 569 |
| Normal | Authentication-2 | 324 | 245 | N/A | 569 |
| WCT\_RCOFF\_GOFF | Attack | DoS | 2000 | 2000 | 2000 | 6000 |
| Authentication-1 | 324 | 245 | 213 | 782 |
| Normal | Authentication-2 | 324 | 245 | 213 | 782 |
| WCT\_RCOFF\_GON | Attack | DoS | 1 | 9 | 19 | 29 |
| Authentication-1 | 324 | 245 | 213 | 782 |
| Normal | Authentication-2 | 324 | 245 | 213 | 782 |
| WCT\_RCON\_GOFF | Attack | DoS | N/A | 2000 | 2000 | 4000 |
| Authentication-1 | N/A | 245 | 213 | 458 |
| Normal | Authentication-2 | N/A | 245 | 213 | 458 |
| WCT\_RCON\_GON | Attack | DoS | 0 | 0 | 19 | 19 |
| Authentication-1 | 324 | 245 | 213 | 782 |
| Normal | Authentication-2 | 324 | 245 | 213 | 782 |
| WET\_RCOFF\_GOFF | Attack | DoS | 2000 | 2000 | 2000 | 6000 |
| Authentication-1 | 324 | 245 | 213 | 782 |
| Normal | Authentication-2 | 324 | 245 | 213 | 782 |
| WET\_RCOFF\_GON | Attack | DoS | 1 | 9 | 19 | 29 |
| Authentication-1 | 324 | 245 | 213 | 782 |
| Normal | Authentication-2 | 324 | 245 | 213 | 782 |
| WET\_RCON\_GOFF | Attack | DoS | N/A | N/A | 2000 | 2000 |
| Authentication-1 | N/A | N/A | 213 | 213 |
| Normal | Authentication-2 | N/A | N/A | 213 | 213 |
| WET\_RCON\_GON | Attack | DoS | 2000 | 2000 | 2000 | 6000 |
| Authentication-1 | 324 | 245 | 213 | 782 |
| Normal | Authentication-2 | 324 | 245 | 213 | 782 |
| WID\_RCOFF\_GOFF | Attack | DoS | 2000 | 2000 | 2000 | 6000 |
| Authentication-1 | 324 | 245 | 213 | 782 |
| Normal | Authentication-2 | 324 | 245 | 213 | 782 |
| WID\_RCOFF\_GON | Attack | DoS | 1 | 9 | 19 | 29 |
| Authentication-1 | 324 | 245 | 213 | 782 |
| Normal | Authentication-2 | 324 | 245 | 213 | 782 |
| WID\_RCON\_GOFF | Attack | DoS | 2000 | 2000 | N/A | 4000 |
| Authentication-1 | 324 | 245 | N/A | 569 |
| Normal | Authentication-2 | 324 | 245 | N/A | 569 |
| WID\_RCON\_GON | Attack | DoS | 0 | 9 | 19 | 28 |
| Authentication-1 | 324 | 245 | 213 | 782 |
| Normal | Authentication-2 | 324 | 245 | 213 | 782 |

Table 3 shows the number of EV authentications processed by the CS and GS and the number of DDoS attacks. In the attack mode, normal EV authentications and DDoS attacks are randomly mixed and race each other for access to the CS and GS. Meanwhile, only normal EVs access the CS and GS for authentication in the normal mode. In the sub-scenario abbreviation field, "CID," "WCT," "WET," and "WID" are described in Table 1, Major Scenarios. "RCOFF" means the attacker performs DDoS attacks toward all CS. In "RCON," the attacker randomly selects the target CS. "GOFF" indicates not applying the Gaussian analysis. "GON," on the other hand, means that the Gaussian analysis is applied. Three CS are used in this experiment, and they are selected or not selected according to the category of the Sub-Scenario. Also, depending on whether the Gaussian analysis is applied, the number of DDoS attacks tends to be very small compared to normal EV authentications.

Table 4. Consumed times for the simulation

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Sub-Scenario Abbreviation | Attack Mode (second) | Normal Mode (seccond) | Total time (second) | Time Difference between Attack and Normal Modes | |
| Second | Ratio |
| CID\_RCOFF\_GOFF | 382.171 | 404.289 | 786.46 | 22.117 | 2.819% |
| CID\_RCOFF\_GON | 29.238 | 53.209 | 82.447 | 23.971 | 29.074% |
| CID\_RCON\_GOFF | 211.574 | 233.854 | 445.428 | 22.279 | 5.001% |
| CID\_RCON\_GON | 28.092 | 51.892 | 79.984 | 23.8 | 29.755% |
| WCT\_RCOFF\_GOFF | 382.849 | 403.764 | 732.613 | 20.914 | 2.854% |
| WCT\_RCOFF\_GON | 28.588 | 51.877 | 80.465 | 23.289 | 28.943% |
| WCT\_RCON\_GOFF | 203.895 | 226.87 | 430.765 | 22.974 | 5.333% |
| WCT\_RCON\_GON | 27.329 | 52.037 | 79.366 | 24.708 | 31.131% |
| WET\_RCOFF\_GOFF | 362.421 | 384.445 | 746.866 | 22.023 | 2.948% |
| WET\_RCOFF\_GON | 28.747 | 51.751 | 80.498 | 23.004 | 28.577 |
| WET\_RCON\_GOFF | 185.92 | 209.207 | 395.127 | 23.287 | 5.893% |
| WET\_RCON\_GON | 27.461 | 52.342 | 79.803 | 24.88 | 31.176 |
| WID\_RCOFF\_GOFF | 383.164 | 403.756 | 786.92 | 20.592 | 2.616% |
| WID\_RCOFF\_GON | 28.916 | 53.781 | 82.697 | 24.864 | 30.066% |
| WID\_RCON\_GOFF | 220.559 | 244.592 | 465.151 | 24.033 | 5.166% |
| WID\_RCON\_GON | 27.553 | 52.198 | 79.751 | 24.645 | 30.902% |

Table 4 shows the simulation time taken in each attack scenario. The average time difference between the attack and normal modes is 23.211 seconds. Depending on each scenario, the total time and ratio vary to some extent. The time difference between all the attack scenarios in seconds is about 23, similar to the average. This means that the time scaling technique [1] minimizes the time difference between the attack and normal modes. However, many multi-threads and multi-processes must be generated to create multiple EVs and CS and communicate with each other. Consequently, an unavoidable delay from the system may occur. In Table 4, the average value in the time difference between the normal and attack modes represents the system overhead that inevitably occurs when performing the simulation.

Figure 3. Difference comparison in the simulation time and ratio in Table 4

Figure 3 shows the time difference between the attack and normal mode simulations in Table 4 and the ratio of the difference. The below expression calculates the ratio.

* .

The ratio value varies greatly depending on whether the Gaussian analysis is activated or deactivated. However, the seconds between the attack and normal modes are relatively small regardless of whether the Gaussian analysis is applied. The features collected from the simulation are processed through feature engineering procedures before being used in ML. As shown in Table 1, the feature types are divided into Perf TOP, Perf STAT, and Time Delta, so the engineering processes are divided into three parts independently. First, as seen in Table 1, Perf STAT is divided into instruction, cycle, and branch categories. Also, since there are three CS and a GS in Table 3, data points are divided into each CS or the GS. The size of the separated data points differs according to the CS and GS types and those categories. Second, Perf TOP provides various symbols representing the overhead of kernel processes [1]. These symbols are of different types and sizes for each CS and GS. The sizes of the data points belonging to the CS or GS are different according to the type of the symbols. The Time Delta has different data point sizes depending on the CS and GS types. Since the data point sizes of the Perf TOP, Perf STAT, and Time Delta vary, the sizes must be the same to be used as ML features. Perf STAT and Perf TOP are measured at 1-second intervals through the PMU.

### Measuring Consumed Resources

The Perf STAT measures CPU cycles, general instructions, and branch instructions consumed in the EV-CS DDoS simulator. Systems used for CS and GS can use CPUs of various performances. If the Perf STAT data is extracted with the PMU in a CPU with a specific performance, the Perf STAT results for systems with CPUs with different performances may differ. Because of this, the Perf STAT dataset created in one system does not show consistent ML feature characteristics in other systems. However, we guarantee consistent measurements regardless of system performance since we measure consumed cycles, branch instructions, and general instructions. If the same program is profiled, these consumed system resources are absolute values ​​unaffected by different system performance.

Figure 4. Perf STAT benchmarking results of different CPUs on Sysbench

Figure 4 shows the benchmarking results for Perf STAT on CPUs with different clocks. We used Sysbench [38] as the benchmarking program at version 1.0.2 and the Perf at version 5.15.0.76.83 in the linux-tool-common. In Sysbench, the CPU's prime factorization ability was tested, the maximum prime number was 10000000, and the number of threads was set to 8. This number of threads is the same as the number of Intel i5 8265U logical cores, the CPU used in this experiment. The CPU clocks are 0.898 GHz, 1.796 GHz, and 2.693 GHz, respectively, doubling and tripling from 0.898 GHz. These CPU clocks were each downclocked on that CPU.

Table 5. Difference comparison on the Perf STAT benchmark

|  |  |  |  |
| --- | --- | --- | --- |
| Feature  Difference | Cycles | Instructions | Branches |
| Standard Deviation (SD) | 500453104.4 | 256310282.2 | 44138751.69 |
| Arithmetic Average (AA) | 446,839,990,078 | 154,472,066,987 | 42,145,946,398 |
|  | 0.0011199828025971 | 0.0016592662168596 | 0.0010472834391517 |

Table 5 shows a breakdown of the Perf STAT benchmarking results in Table 4. SD and AA compare the Perf STAT difference between the values ​​of different CPU clocks for each feature type. Since SD divided by AA is close to zero, it is proved that the CPU clock does not affect the result of Perf STAT.

Figure 5. Benchmarking times spent in different CPUs in Figure 4

Figure 5 shows the time taken in seconds for the Perf STAT benchmarking measurement of Figure 4. At 0.898 GHz CPU clock, 63.626 seconds were consumed, about 55% of the total; at 1.796 GHz CPU clock, 31.538 seconds were consumed, about 27%; and at 2.693 GHz CPU clock, 20.93 seconds, were consumed about 18%. Based on the CPU clock of 0.898 GHz, the other clocks show that each took 2x and 3x longer.

Table 6. Feature combination of the Perf STAT and Time Delta [1]

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Index | 1 | 2 | 3 | 4 | 5 |
| Combination | branch | cycle | instruction | Time Delta | branch, cycle |
| Index | 6 | 7 | 8 | 9 | 10 |
| Combination | branch, instruction | branch, Time Delta | cycle, instruction | cycle, Time Delta | instruction, Time Delta |
| Index | 11 | 12 | 13 | 14 | 15 |
| Combination | branch, cycle, instruction | branch, cycle, Time Delta | branch, instruction, Time Delta | cycle, instruction, Time Delta | branch, cycle, instruction, Time Delta |

Table 6 shows the combination of all features in the Perf STAT. From four basic features, Instruction, cycle, branch, and Time Delta, fifteen cases are calculated when the features are combined. The total number of feature combinations is calculated as follows:

* the number of the total features.

Table 7. Feature information of the Perf STAT and Time Delta on the CS [1]

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Sub-Scenario Abbreviation | Category | Mode | CS ID | | | | | | | | | | | |
| 2-39-89-25 | | | | 2-39-139-28 | | | | 2-39-131-30 | | | |
| Feature Index in Table 6 | | | | | | | | | | | |
| 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 |
| CID\_RCOFF\_GOFF | Feature Size | Attack | 3720 | 3720 | 3720 | 2212 | 3774 | 3774 | 3774 | 2323 | 3762 | 3762 | 3762 | 2244 |
| Normal | 3569 | 3569 | 3569 | 213 | 3677 | 3677 | 3677 | 324 | 3647 | 3647 | 3647 | 245 |
| Sampling Resolution | Attack | 9.733 | 9.733 | 9.733 | 5.787 | 9.875 | 9.875 | 9.875 | 6.078 | 9.843 | 9.843 | 9.843 | 5.871 |
| Normal | 8.827 | 8.827 | 8.827 | 0.526 | 9.094 | 9.094 | 9.094 | 0.801 | 9.02 | 9.02 | 9.02 | 0.606 |
| CID\_RCOFF\_GON | Feature Size | Attack | 255 | 255 | 255 | 231 | 282 | 282 | 282 | 324 | 260 | 260 | 260 | 253 |
| Normal | 434 | 434 | 434 | 213 | 497 | 497 | 497 | 324 | 459 | 459 | 459 | 245 |
| Sampling Resolution | Attack | 8.721 | 8.721 | 8.721 | 7.9 | 9.644 | 9.644 | 9.644 | 11.081 | 8.892 | 8.892 | 8.892 | 8.653 |
| Normal | 8.156 | 8.156 | 8.156 | 4.003 | 9.34 | 9.34 | 9.34 | 6.089 | 8.626 | 8.626 | 8.626 | 4.604 |
| CID\_RCON\_GOFF | Feature Size | Attack | 2044 | 2044 | 2044 | 2212 | N/A | N/A | N/A | N/A | 2049 | 2049 | 2049 | 2244 |
| Normal | 2040 | 2040 | 2040 | 213 | N/A | N/A | N/A | N/A | 2092 | 2092 | 2092 | 245 |
| Sampling Resolution | Attack | 9.66 | 9.66 | 9.66 | 10.454 | N/A | N/A | N/A | N/A | 9.684 | 9.684 | 9.684 | 10.606 |
| Normal | 8.723 | 8.723 | 8.723 | 0.91 | N/A | N/A | N/A | N/A | 8.945 | 8.945 | 8.945 | 1.047 |
| CID\_RCON\_GON | Feature Size | Attack | N/A | N/A | N/A | N/A | 274 | 274 | 274 | 323 | 240 | 240 | 240 | 244 |
| Normal | N/A | N/A | N/A | N/A | 484 | 484 | 484 | 324 | 449 | 449 | 449 | 245 |
| Sampling Resolution | Attack | N/A | N/A | N/A | N/A | 9.753 | 9.753 | 9.753 | 11.497 | 8.543 | 8.543 | 8.543 | 8.685 |
| Normal | N/A | N/A | N/A | N/A | 9.326 | 9.326 | 9.326 | 6.243 | 8.652 | 8.652 | 8.652 | 4.721 |
| WCT\_RCOFF\_GOFF | Feature Size | Attack | 3730 | 3730 | 3730 | 2212 | 3781 | 3781 | 3781 | 2323 | 3753 | 3753 | 3753 | 2244 |
| Normal | 3565 | 3565 | 3565 | 213 | 3676 | 3676 | 3676 | 324 | 3647 | 3647 | 3647 | 245 |
| Sampling Resolution | Attack | 9.742 | 9.742 | 9.742 | 5.777 | 9.875 | 9.875 | 9.875 | 6.067 | 9.802 | 9.802 | 9.802 | 5.861 |
| Normal | 8.829 | 8.829 | 8.829 | 0.527 | 9.104 | 9.104 | 9.104 | 0.802 | 9.032 | 9.032 | 9.032 | 0.606 |
| WCT\_RCOFF\_GON | Feature Size | Attack | 245 | 245 | 245 | 231 | 277 | 277 | 277 | 324 | 252 | 252 | 252 | 253 |
| Normal | 409 | 409 | 409 | 213 | 481 | 481 | 481 | 324 | 437 | 437 | 437 | 245 |
| Sampling Resolution | Attack | 8.569 | 8.569 | 8.569 | 8.08 | 9.689 | 9.689 | 9.689 | 11.333 | 8.814 | 8.814 | 8.814 | 8.849 |
| Normal | 7.883 | 7.883 | 7.883 | 4.105 | 9.271 | 9.271 | 9.271 | 6.245 | 8.423 | 8.423 | 8.423 | 4.722 |
| WCT\_RCON\_GOFF | Feature Size | Attack | 1989 | 1989 | 1989 | 2212 | N/A | N/A | N/A | N/A | 1994 | 1994 | 1994 | 2244 |
| Normal | 1975 | 1975 | 1975 | 213 | N/A | N/A | N/A | N/A | 2026 | 2026 | 2026 | 245 |
| Sampling Resolution | Attack | 9.754 | 9.754 | 9.754 | 10.848 | N/A | N/A | N/A | N/A | 9.779 | 9.779 | 9.779 | 11.005 |
| Normal | 8.7 | 8.7 | 8.7 | 0.938 | N/A | N/A | N/A | N/A | 8.93 | 8.93 | 8.93 | 1.079 |
| WCT\_RCON\_GON | Feature Size | Attack | 229 | 229 | 229 | 231 | 262 | 262 | 262 | 323 | 241 | 241 | 241 | 244 |
| Normal | 409 | 409 | 409 | 213 | 475 | 475 | 475 | 324 | 435 | 435 | 435 | 245 |
| Sampling Resolution | Attack | 8.379 | 8.379 | 8.379 | 8.452 | 9.586 | 9.586 | 9.586 | 11.818 | 8.818 | 8.818 | 8.818 | 8.928 |
| Normal | 7.859 | 7.859 | 7.859 | 4.093 | 9.128 | 9.128 | 9.128 | 6.226 | 52.037 | 8.359 | 8.359 | 4.708 |
| WET\_RCOFF\_GOFF | Feature Size | Attack | 3523 | 3523 | 3523 | 2212 | 3580 | 3580 | 3580 | 2323 | 3546 | 3546 | 3546 | 2244 |
| Normal | 3395 | 3395 | 3395 | 213 | 3501 | 3501 | 3501 | 324 | 3455 | 3455 | 3455 | 245 |
| Sampling Resolution | Attack | 9.72 | 9.72 | 9.72 | 6.103 | 9.878 | 9.878 | 9.878 | 6.409 | 9.784 | 9.784 | 9.784 | 6.191 |
| Normal | 8.83 | 8.83 | 8.83 | 0.554 | 9.106 | 9.106 | 9.106 | 0.842 | 8.986 | 8.986 | 8.986 | 0.637 |
| WET\_RCOFF\_GON | Feature Size | Attack | 248 | 248 | 248 | 231 | 280 | 280 | 280 | 324 | 256 | 256 | 256 | 253 |
| Normal | 420 | 420 | 420 | 213 | 483 | 483 | 483 | 324 | 448 | 448 | 448 | 245 |
| Sampling Resolution | Attack | 8.626 | 8.626 | 8.626 | 8.035 | 9.74 | 9.74 | 9.74 | 11.27 | 8.905 | 8.905 | 8.905 | 8.8 |
| Normal | 8.115 | 8.115 | 8.115 | 4.115 | 9.333 | 9.333 | 9.333 | 6.26 | 8.656 | 8.656 | 8.656 | 4.734 |
| WET\_RCON\_GOFF | Feature Size | Attack | 1831 | 1831 | 1831 | 2212 | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A |
| Normal | 1818 | 1818 | 1818 | 213 | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A |
| Sampling Resolution | Attack | 9.848 | 9.848 | 9.848 | 11.897 | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A |
| Normal | 8.689 | 8.689 | 8.689 | 1.018 | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A |
| WET\_RCON\_GON | Feature Size | Attack | 224 | 224 | 224 | 212 | 267 | 267 | 267 | 324 | 242 | 242 | 242 | 253 |
| Normal | 426 | 426 | 426 | 213 | 491 | 491 | 491 | 324 | 446 | 446 | 446 | 245 |
| Sampling Resolution | Attack | 8.156 | 8.156 | 8.156 | 7.72 | 9.722 | 9.722 | 9.722 | 11.798 | 27.461 | 8.812 | 8.812 | 9.213 |
| Normal | 8.138 | 8.138 | 8.138 | 4.069 | 9.38 | 9.38 | 9.38 | 6.19 | 8.52 | 8.52 | 8.52 | 4.68 |
| WID\_RCOFF\_GOFF | Feature Size | Attack | 3724 | 3724 | 3724 | 2212 | 3769 | 3769 | 3769 | 2323 | 3744 | 3744 | 3744 | 2244 |
| Normal | 3567 | 3567 | 3567 | 213 | 3679 | 3679 | 3679 | 324 | 3652 | 3652 | 3652 | 245 |
| Sampling Resolution | Attack | 9.719 | 9.719 | 9.719 | 5.772 | 9.836 | 9.836 | 9.836 | 6.062 | 9.771 | 9.771 | 9.771 | 5.856 |
| Normal | 8.834 | 8.834 | 8.834 | 0.527 | 9.111 | 9.111 | 9.111 | 0.802 | 9.045 | 9.045 | 9.045 | 0.606 |
| WID\_RCOFF\_GON | Feature Size | Attack | 244 | 244 | 244 | 231 | 280 | 280 | 280 | 324 | 243 | 243 | 243 | 253 |
| Normal | 432 | 432 | 432 | 213 | 504 | 504 | 504 | 324 | 460 | 460 | 460 | 245 |
| Sampling Resolution | Attack | 8.438 | 8.438 | 8.438 | 7.988 | 9.683 | 9.683 | 9.683 | 11.204 | 8.403 | 8.403 | 8.403 | 8.749 |
| Normal | 8.032 | 8.032 | 8.032 | 3.96 | 9.371 | 9.371 | 9.371 | 6.024 | 8.553 | 8.553 | 8.553 | 4.555 |
| WID\_RCON\_GOFF | Feature Size | Attack | N/A | N/A | N/A | N/A | 2171 | 2171 | 2171 | 2323 | 2125 | 2125 | 2125 | 2244 |
| Normal | N/A | N/A | N/A | N/A | 2226 | 2226 | 2226 | 324 | 2195 | 2195 | 2195 | 245 |
| Sampling Resolution | Attack | N/A | N/A | N/A | N/A | 9.843 | 9.843 | 9.843 | 10.532 | 9.634 | 9.634 | 9.634 | 10.174 |
| Normal | N/A | N/A | N/A | N/A | 9.1 | 9.1 | 9.1 | 1.324 | 8.974 | 8.974 | 8.974 | 1.001 |
| WID\_RCON\_GON | Feature Size | Attack | 238 | 238 | 238 | 231 | 267 | 267 | 267 | 323 | 242 | 242 | 242 | 253 |
| Normal | 410 | 410 | 410 | 213 | 478 | 478 | 478 | 324 | 436 | 436 | 436 | 245 |
| Sampling Resolution | Attack | 8.637 | 8.637 | 8.637 | 8.383 | 9.69 | 9.69 | 9.69 | 11.722 | 8.783 | 8.783 | 8.783 | 9.182 |
| Normal | 7.854 | 7.854 | 7.854 | 4.08 | 9.157 | 9.157 | 9.157 | 6.207 | 8.352 | 8.352 | 8.352 | 4.693 |

Table 7 shows the information on the Perf STAT and Time Delta features of CS under the attack scenarios. The information indicates the feature size and sampling resolution used in the DDoS attacks or normal EV authentication modes. In the random CS mode ("RCON or RCOFF"), feature information of CS not selected as attack targets does not exist. In the Gaussian Analysis-enabled mode ("GON"), the number of the Perf STAT features collected by the PMU is greater than that in the disabled mode ("GOFF"). The feature size difference of the time is very large depending on whether the Gaussian Mode is on or off. The sampling resolution is calculated by the expression below.

* in Tables 4 and 7.

The higher the value of the sampling resolution, the more suitable it is for use as an ML feature, and the smaller the value, the less suitable it is.

Table 8. Feature information of the Perf STAT on the GS [1]

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Sub-Scenario Abbreviation | Category | Mode | GS | | |
| Feature Index in Table 6 | | |
| 1 | 2 | 3 |
| CID\_RCOFF\_GOFF | Feature Size | Attack | 3739 | 3739 | 3739 |
| Normal | 2464 | 2464 | 2464 |
| Sampling Resolution | Attack | 9.783 | 9.783 | 9.783 |
| Normal | 6.094 | 6.094 | 6.094 |
| CID\_RCOFF\_GON | Feature Size | Attack | 2464 | 2464 | 2464 |
| Normal | 421 | 421 | 421 |
| Sampling Resolution | Attack | 84.273 | 84.273 | 84.273 |
| Normal | 7.912 | 7.912 | 7.912 |
| CID\_RCON\_GOFF | Feature Size | Attack | 2053 | 2053 | 2053 |
| Normal | 1474 | 1474 | 1474 |
| Sampling Resolution | Attack | 9.703 | 9.703 | 9.703 |
| Normal | 6.303 | 6.303 | 6.303 |
| CID\_RCON\_GON | Feature Size | Attack | 236 | 236 | 236 |
| Normal | 418 | 418 | 418 |
| Sampling Resolution | Attack | 8.4 | 8.4 | 8.4 |
| Normal | 8.055 | 8.055 | 8.055 |
| WCT\_RCOFF\_GOFF | Feature Size | Attack | 3729 | 3729 | 3729 |
| Normal | 2478 | 2478 | 2478 |
| Sampling Resolution | Attack | 9.74 | 9.74 | 9.74 |
| Normal | 6.137 | 6.137 | 6.137 |
| WCT\_RCOFF\_GON | Feature Size | Attack | 242 | 242 | 242 |
| Normal | 411 | 411 | 411 |
| Sampling Resolution | Attack | 8.464 | 8.464 | 8.464 |
| Normal | 7.922 | 7.922 | 7.922 |
| WCT\_RCON\_GOFF | Feature Size | Attack | 3729 | 3729 | 3729 |
| Normal | 2478 | 2478 | 2478 |
| Sampling Resolution | Attack | 9.74 | 9.74 | 9.74 |
| Normal | 6.137 | 6.137 | 6.137 |
| WCT\_RCON\_GON | Feature Size | Attack | 235 | 235 | 235 |
| Normal | 411 | 411 | 411 |
| Sampling Resolution | Attack | 8.598 | 8.598 | 8.598 |
| Normal | 7.898 | 7.898 | 7.898 |
| WET\_RCOFF\_GOFF | Feature Size | Attack | 1996 | 1996 | 1996 |
| Normal | 2344 | 2344 | 2344 |
| Sampling Resolution | Attack | 5.507 | 5.507 | 5.507 |
| Normal | 6.097 | 6.097 | 6.097 |
| WET\_RCOFF\_GON | Feature Size | Attack | 244 | 244 | 244 |
| Normal | 418 | 418 | 418 |
| Sampling Resolution | Attack | 8.487 | 8.487 | 8.487 |
| Normal | 8.077 | 8.077 | 8.077 |
| WET\_RCON\_GOFF | Feature Size | Attack | 1105 | 1105 | 1105 |
| Normal | 1394 | 1394 | 1394 |
| Sampling Resolution | Attack | 5.943 | 5.943 | 5.943 |
| Normal | 6.663 | 6.663 | 6.663 |
| WET\_RCON\_GON | Feature Size | Attack | 227 | 227 | 227 |
| Normal | 227 | 227 | 227 |
| Sampling Resolution | Attack | 8.266 | 8.266 | 8.266 |
| Normal | 4.336 | 4.336 | 4.336 |
| WID\_RCOFF\_GOFF | Feature Size | Attack | 3735 | 3735 | 3735 |
| Normal | 2553 | 2553 | 2553 |
| Sampling Resolution | Attack | 9.747 | 9.747 | 9.747 |
| Normal | 6.323 | 6.323 | 6.323 |
| WID\_RCOFF\_GON | Feature Size | Attack | 243 | 243 | 243 |
| Normal | 454 | 454 | 454 |
| Sampling Resolution | Attack | 8.403 | 8.403 | 8.403 |
| Normal | 8.441 | 8.441 | 8.441 |
| WID\_RCON\_GOFF | Feature Size | Attack | 2124 | 2124 | 2124 |
| Normal | 1551 | 1551 | 1551 |
| Sampling Resolution | Attack | 9.63 | 9.63 | 9.63 |
| Normal | 6.341 | 6.341 | 6.341 |
| WID\_RCON\_GON | Feature Size | Attack | 250 | 250 | 250 |
| Normal | 415 | 415 | 415 |
| Sampling Resolution | Attack | 9.073 | 9.073 | 9.073 |
| Normal | 7.95 | 7.95 | 7.95 |

Table 8 shows the feature information for the Perf STAT collected from the GS, like Table 7. The Time Delta is not separately used in the GS, but the same data measured based on the CS are used. In Table 7, the CS consist of three stations, unlike the GS, so the Perf STAT and Time Delta features differ, although they are the same feature types.

## Feature Transformation

The features of the same type extracted from different CS must be integrated into one feature type to be used in ML. Since features of the same type are extracted from different CS, each feature's size may not be identical. If the size of each feature is different, a loss of a specific part of the feature occurs during the integration process because the feature size must be set to be the same. Therefore, we calculate the loss rate for the Perf STAT and Time Delta extracted from the CS. Different feature sizes must shrink or increase each other to make them the same size. In the case of increasing feature size, a small feature size has to be artificially increased through a regression analysis [27].

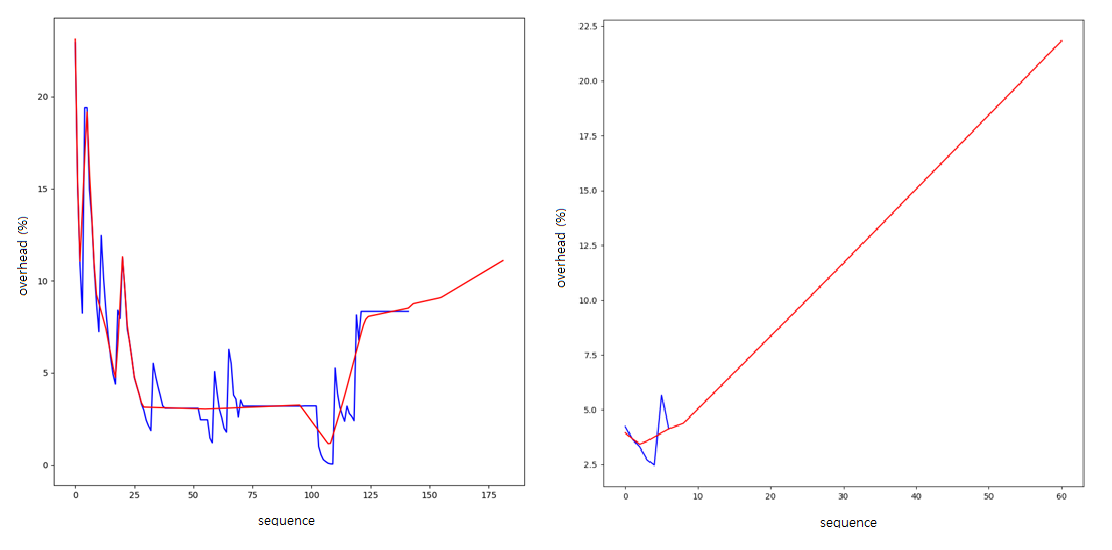


Figure 6. Data point generation based on regression analysis

Figure 6 shows that new data points are created by applying regression analysis on the data points of a feature extracted from Perf TOP. The blue line represents the original data points, and the red line indicates the new ones created through the regression analysis. The number of data points in the graph on the left is relatively plenty to the other graph. The original and new data points have similar values ​​to some extent. However, when the original data points are sparse, as seen in the graph on the right, newly created data points tend to diverge with completely different values. Some of the features used in this study have extremely large differences in size. In this regard, a method [27] of increasing the size of a feature by applying the regression analysis is unsuitable for this study.

Methods for reducing the size of features are typically divided into sampling with replacement [28] and sampling without replacement [29]. The former in sampling put the extracted data back into the sample, so the same data is likely to be selected. In the latter, extracted data is not added to the sample again, so the sampled data is unlikely to be identical. In this study, we adopt the non-replacement sampling method [29] for reducing feature size, which has no possibility of data duplication. The combined loss rate refers to the loss of data points in integrating each sub-feature of the same type on the CS. Among the sub-features to be integrated, the loss rate is obtained by averaging the difference of sampling resolutions between a feature of the smallest data point size and other sub-features. The calculation of the Combined Loss Rate (CLR) is below.

* : sub-feature count, sampling resolution.

### Feature Size Synchronization by Down Sampling

A large-size feature must be reduced to the same size as a small-size feature for the feature combination. When the size of a feature is reduced, a loss of a certain portion of the feature is unavoidable. Data pointers are selected randomly by size to be reduced from the large feature [29]. This random extraction method has one problem. Even though the extracted data points are randomly extracted, there is no guarantee that the sample data of the feature are uniformly extracted. In other words, the frequency of sampling data points from a specific sample area may be relatively high. Therefore, when reducing the size of a feature, a method of uniformly and randomly extracting data points is required.

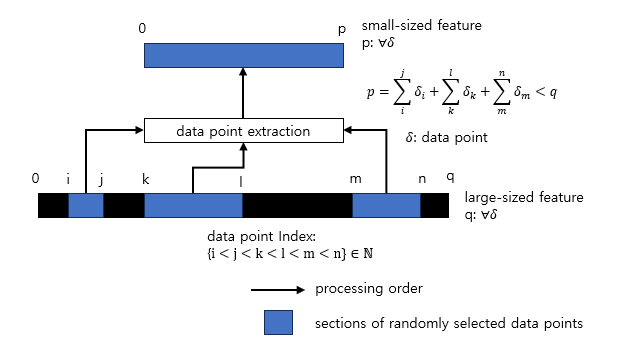


Figure 7. Data point extraction from a large-sized feature to a small-sized one [29, 30]

Figure 7 shows the non-replacement extraction method [29] randomly from a large-sized feature to a small-sized one. The blue parts show the possibility of forming biased clusters in specific parts, even though features are supposed to be randomly extracted. If only the specific parts of a feature to be reduced are mainly extracted, the characteristics of the feature cannot be fully preserved.

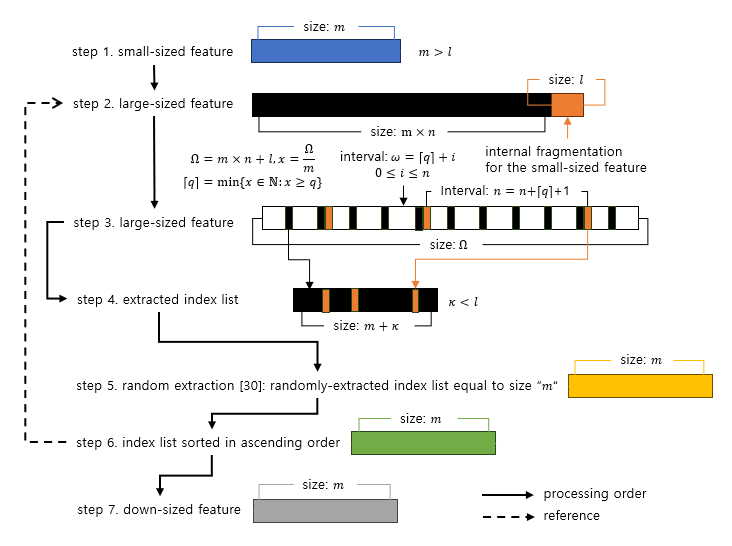


Figure 8. Feature size reduction process

Figure 8 shows the feature downsizing methods proposed in this paper from Steps 1 to 7. In steps 1 and 2, the small-sized feature is divisible by an integer multiple of the size "" of the large-sized feature. However, the orange portion is not divisible by the integer multiple because the size "" is smaller than the size "." This indivisible part is internal fragmentation. In steps 3 and 4, indices pointing to data points in the large-size feature are extracted at specific intervals. Additional indices may remain from the feature division between the small and large features. In this regard, "" additional indexes are selected more than "" indexes. Steps 5 and 6 show the generation of a new list by randomly selecting "" indexes among the "" indexes extracted in Step 4. Randomly selecting "" indices ensures that a list equal to the size "" to be reduced is created. The selected indices are sorted in ascending order to extract data points from the feature of Step 2. A new list is constructed from the "" data points extracted in step 7. The pseudo-code for Figure 6 is:

Table 9. The list of the symbols used in Figure 6

|  |  |  |  |
| --- | --- | --- | --- |
| Symbol | Explanation | Symbol | Explanation |
|  | Small-sized feature list |  | The remainder of the large-sized feature divided by the small-sized feature |
|  | Down-sized feature list |  | The sum of |
| 𝑚 | Feature size |  |  |
| 𝑛 | Integer multiple of 𝑚 |  | Data point index |
| 𝛺 | Feature size |  | The element of a set |
| 𝑙 | Feature size |  | The result of dividing the large-sized feature by the small-sized one |
|  | The quotient of the large-sized feature divided by the small-sized feature |  | Large-sized feature list |
|  | Index list |  |  |

텍스트, 폰트, 친필, 영수증이(가) 표시된 사진

자동 생성된 설명

Figure 9. Pseudo code of the proposed feature down-sizing method

Table 9 describes the symbols used in Figure 8 and the above pseudo-code. Figure 9 is the pseudo-code for the feature downsizing technique proposed in this paper. The performance test of the proposed downsizing technique was conducted on various feature sizes.

Figure 10. Original sample data to be reduced

Figure 11. Result reduced to a small number of data points

Figure 12. Result reduced to a large number of data points

Figure 10 shows 9500 data points generated through the objective function of . Figure 11 shows the result of downsizing the data points in Figure 10 to 10 data points. Figure 12 is the result of downsizing the data points in Figure 10 to 1000 data points. Figures 11 and 12 show that the green data are only randomly extracted and sorted when downsizing the features. The other red data shows the result of applying all the steps in Figures 8 and 9. In Figure 12, when the number of data samples is large, a few distortions occur compared to the original samples in Figure 10. However, in Figure 11, when the data is very small, the degree of distortion becomes very large.

Figure 13. Original sample data to be reduced

Figure 14. Result reduced to a small number of data points

Figure 15. Result reduced to a large number of data points

Figure 13 shows sample data generated through an objective function below.

* .

These sample data are downsized to 1000 data points in Figures 14 and 15, respectively. Figure 14 randomly extracts the red data points with sorting during downsizing samples from Figure 13. The green data points represent the reduced samples through the downsizing technique proposed in this paper. In Figure 15, the red data points indicate that a sorting process is not implemented after randomly extracting data from the original downsizing samples in Figure 13. The green data shows the proposed downsizing technique applied. The random algorithm [30] used in this feature downsizing is a Python library that provides an official random function and is similar to the random extraction function used in the sampling without replacement [29]. As demonstrated in these figures, the feature downsizing method proposed in this paper is almost identical to the shape of the original samples after downsizing, regardless of the number of data points.

Table 9. Comparison of existing sampling methods [31]

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Algorithm Name | Sampling without replacement | Time Complexity | Data Extraction Method from an Array | Randomly Element Shuffling Method |
| Fisher-Yates Sampler | Yes |  | Simple Element swapping | Uniform random generator based on Fisher-Yates sampling |
| Sparse Fisher-Yates Sampler | Yes |  | Hash-based element swapping |
| Membership checking | Yes |  | Non-overlapping Hash-based element swapping |
| Pre-initialized FY | Yes |  | Element swapping with undoing permutation in reverse order |
| Ours | Yes |  | Index extraction method that maximizes equal spacing of a downsizing feature | Hybrid random generator |

Table 9 compares our proposed key algorithm for feature downsizing and similar algorithms. The "Fisher" algorithm is a simple way to extract and swap elements from an array without duplicates. The "Sparse Fisher-Yates " algorithm tags some elements of an array with a hash and then extracts only the tagged elements. The “Membership checking” algorithm also extracts the elements by hashing the indices of the array. However, unlike the “Sparse Fisher-Yates” algorithm, the indices are repeatedly extracted until a selected index does not overlap with a hash table key. When swapping array elements, the “Pre-initialized FY” algorithm repeats the permutation, applying the transposition in reverse order. The time complexities of the listed sampling algorithms are almost similar, so there is no significant difference in performance. All the algorithms are non-replacement extraction methods and internally shuffle the indices using the same random generator [30,32] except ours. Thus, the algorithms described in this paper [31] rely on the random generator to make a uniform distribution when sampling the data. The feature downsizing technique proposed in this paper is demonstrated as follows. The superiority of the feature downsizing technique proposed in this paper is demonstrated as follows.

#### Proof

def. In Figure 8, let . As the graph is non-linear, assume that pieces of data fit with an -order polynomial equation [33]. can be approximated by , . Let a residual . A Sum of Squared Error (SSR) [34] is expressed as . s.t., . We can maximize the approximation from to by finding , and substituting it into . cf.. Since this equation can be expressed as a matrix, Gaussian elimination [35] can be applied. s.t., . Through this matrix operation, we can obtain }. Since for , the polynomial regression equation is . The matrix used in this research is . Since this matrix is ​​symmetric, only the diagonal and the other half elements can be considered for simple calculation. Let . cond., , cond., : cofactor. We can separate the above matrix equation into . s.t., . Q.E.D., . We can obtain the coefficient matrix from this proven matrix equation. As mentioned earlier, the degree of as a control group and the degree of as an experimental group with polynomial regression are the same 2. As a result, a second-order objective function is generated from the obtained coefficient values. Let the new objective function be . The function will generate values ​​that are as close as possible in the form of . i.e., . By comparing the difference between the result values ​​of these two functions of the same size, we can determine whether they are similar. Root Mean Square Error (RMSE) [36] and R-square [37] calculate the difference between observed and estimated data for a particular distribution. The closer the calculated value is to 0, the more similar the two functions are. Conversely, the larger the value, the more different the two functions are. s.t.,

Table 10. Polynomial regression coefficient list

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Estimated Objective Function Prototype | |  | | |
| Down-Sampling Size | Feature Extraction Method | Coefficient Type | | |
|  |  |  |
| 10 | URE | 9021.879 | 11196.552 | 8624.873 |
| Ours | 10000.0 | 0 | 0 |
| Direct PNLR | 0.9999999999999998 | -1.6485010829929417e-15 | 1.4210854715202004e-14 |
| 110 | URE | 92.052 | -701.357 | -4064.699 |
| Ours | 87.414 | -519.43 | 6483.024 |
| Direct PNLR | 1.0 | 2.865202933399981e-14 | -1.3642420526593924e-12 |
| 210 | URE | 22.014 | 75.517 | -4482.615 |
| Ours | 22.326 | 101.451 | -1968.324 |
| Direct PNLR | 1.0000000000000002 | -5.941123857667242e-14 | 1.8189894035458565e-12 |
| 310 | URE | 11.39 | -387.823 | 11046.025 |
| Ours | 10.288 | 57.98 | -413.028 |
| Direct PNLR | 1.0000000000000004 | -1.173240081372717e-13 | 3.637978807091713e-12 |
| 410 | URE | 5.868 | 45.939 | 135.197 |
| Ours | 6.144 | -62.034 | 1182.189 |
| Direct PNLR | 1.0000000000000002 | -4.6488184421653605e-14 | -7.275957614183426e-12 |
| 510 | URE | 3.854 | -12.242 | -2066.324 |
| Ours | 4.048 | -91.267 | 2049.48 |
| Direct PNLR | 0.9999999999999998 | 1.4046174799773593e-13 | -1.4551915228366852e-11 |
| 610 | URE | 2.725 | -60.574 | 9197.995 |
| Ours | 2.753 | -58.719 | 3684 |
| Direct PNLR | 1.0000000000000007 | -2.8754884431846636e-13 | 0 |
| 710 | URE | 1.975 | -8.136 | -1100.445 |
| Ours | 2.062 | -54.106 | 2227.716 |
| Direct PNLR | 1 | 7.848327969280713e-14 | -2.9103830456733704e-11 |
| 810 | URE | 1.493 | 12.618 | -2174.405 |
| Ours | 1.474 | 40.536 | -2493.418 |
| Direct PNLR | 1 | 4.8690251068147905e-14 | -2.9103830456733704e-11 |
| 910 | URE | 1.209 | 7.061 | -104.234 |
| Ours | 1.203 | 7.588 | -970.983 |
| Direct PNLR | 0.9999999999999996 | 6.282331801894737e-13 | -1.7462298274040222e-10 |

Table 10 shows the regression coefficients of the objective function estimated using the polynomial regression analysis proposed in this study. Unifor Random Extraction (URE) refers to existing feature sampling algorithms reviewed in Table 9. From the distribution of with 1000 original data points, 10-step feature downsizing experiments were conducted. In polynomial regression, the objective function is estimated by recursively calculating the pattern of a certain amount of data; thus, ten-step down-sampling sizes were selected, 100 for each step.

Figure 16. RMSE differences in on various down-sizing samples through URE and our method from the original feature

Figure 16 compares the RMSE values ​​by downsizing features with various sizes after regression analysis on the 1000 original samples. When the number of features is reduced to 10, the performance of the URE sampling method is poor. However, the performance is better because the feature downsizing size does not differ from the original size. Our proposed method proves to preserve data better after downsizing than URE.

Figure 17. RMSE differences in on various down-sizing samples from the original feature

Figure 17 compares RMSE after only regression analysis was performed without downsizing. There is no appreciable error with different feature sizes.

Figure 18. Comparison of R square values between URE and our sampling method

Figure 18 shows the comparison of R square values ​​between our proposed sampling method and the URE sampling method. An R square value is obtained by applying only regression analysis without downsizing from the original . We compared the R square values with other R square values of URE and our methods. Since it is a stacked bar graph, the smaller the colored area, the lower the data loss rate when feature downsizing. In Figure 15, after applying the regression analysis to the original , its RMSE values ​​are all the same. Consequently, the R square value of the regression on original samples without downsizing becomes 1.

## Feature Creation

### Combining Different Features

Table 11. The combined loss rate of CS in the attack scenarios

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Sub-Scenario Abbreviation | Mode | Index in Table 6 | | | | | | | | | | | | | | |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
| CID\_RCOFF\_GOFF | Attack | 0.083 | 0.083 | 0.083 | 0.124 | 0.083 | 0.083 | 2.077 | 0.083 | 2.077 | 2.077 | 0.083 | 2.727 | 2.727 | 2.727 | 3.053 |
| Normal | 0.153 | 0.153 | 0.153 | 0.117 | 0.153 | 0.153 | 4.286 | 0.153 | 4.286 | 4.286 | 0.153 | 5.675 | 5.675 | 5.675 | 6.37 |
| CID\_RCOFF\_GON | Attack | 0.364 | 0.364 | 0.364 | 1.311 | 0.364 | 0.364 | 1.248 | 0.364 | 1.248 | 1.248 | 0.364 | 1.227 | 1.227 | 1.227 | 1.217 |
| Normal | 0.551 | 0.551 | 0.551 | 0.895 | 0.551 | 0.551 | 2.8 | 0.551 | 2.8 | 2.8 | 0.551 | 3.435 | 3.435 | 3.435 | 3.752 |
| CID\_RCON\_GOFF | Attack | 0.011 | 0.011 | 0.011 | 0.075 | 0.011 | 0.011 | 0.44 | 0.011 | 0.44 | 0.44 | 0.011 | 0.297 | 0.297 | 0.297 | 0.226 |
| Normal | 0.111 | 0.111 | 0.111 | 0.068 | 0.111 | 0.111 | 3.996 | 0.111 | 3.996 | 3.996 | 0.111 | 5.305 | 5.305 | 5.305 | 5.959 |
| CID\_RCON\_GON | Attack | 0.605 | 0.605 | 0.605 | 1.406 | 0.605 | 0.605 | 1.076 | 0.605 | 1.076 | 1.076 | 0.605 | 0.919 | 0.919 | 0.919 | 0.84 |
| Normal | 0.337 | 0.337 | 0.337 | 0.761 | 0.337 | 0.337 | 2.514 | 0.337 | 2.514 | 2.514 | 0.337 | 3.099 | 3.099 | 3.099 | 3.391 |
| WCT\_RCOFF\_GOFF | Attack | 0.064 | 0.064 | 0.064 | 0.124 | 0.064 | 0.064 | 2.076 | 0.064 | 2.076 | 2.076 | 0.064 | 2.727 | 2.727 | 2.727 | 3.053 |
| Normal | 0.159 | 0.159 | 0.159 | 0.118 | 0.159 | 0.159 | 4.289 | 0.159 | 4.289 | 4.289 | 0.159 | 5.68 | 5.68 | 5.68 | 6.375 |
| WCT\_RCOFF\_GON | Attack | 0.454 | 0.454 | 0.454 | 1.34 | 0.454 | 0.454 | 1.142 | 0.454 | 1.142 | 1.142 | 0.454 | 1.076 | 1.076 | 1.076 | 1.043 |
| Normal | 0.642 | 0.642 | 0.642 | 0.918 | 0.642 | 0.642 | 2.669 | 0.642 | 2.669 | 2.669 | 0.642 | 3.253 | 3.253 | 3.253 | 3.545 |
| WCT\_RCON\_GOFF | Attack | 0.012 | 0.012 | 0.012 | 0.078 | 0.012 | 0.012 | 0.592 | 0.012 | 0.592 | 0.592 | 0.012 | 0.398 | 0.398 | 0.398 | 0.302 |
| Normal | 0.112 | 0.112 | 0.112 | 0.07 | 0.112 | 0.112 | 3.974 | 0.112 | 3.974 | 3.974 | 0.112 | 5.276 | 5.276 | 5.276 | 5.926 |
| WCT\_RCON\_GON | Attack | 0.548 | 0.548 | 0.548 | 1.28 | 0.548 | 0.548 | 0.951 | 0.548 | 0.951 | 0.951 | 0.548 | 0.817 | 0.817 | 0.817 | 0.75 |
| Normal | 0.589 | 0.589 | 0.589 | 0.916 | 0.589 | 0.589 | 2.635 | 0.589 | 2.635 | 2.635 | 0.589 | 3.209 | 3.209 | 3.209 | 3.495 |
| WET\_RCOFF\_GOFF | Attack | 0.073 | 0.073 | 0.073 | 0.131 | 0.073 | 0.073 | 1.911 | 0.073 | 1.911 | 1.911 | 0.073 | 2.504 | 2.504 | 2.504 | 2.801 |
| Normal | 0.143 | 0.143 | 0.143 | 0.123 | 0.143 | 0.143 | 4.272 | 0.143 | 4.272 | 4.272 | 0.143 | 5.655 | 5.655 | 5.655 | 6.346 |
| WET\_RCOFF\_GON | Attack | 0.463 | 0.463 | 0.463 | 1.333 | 0.463 | 0.463 | 1.194 | 0.463 | 1.194 | 1.194 | 0.463 | 1.147 | 1.147 | 1.147 | 1.124 |
| Normal | 0.586 | 0.586 | 0.586 | 0.921 | 0.586 | 0.586 | 2.753 | 0.586 | 2.753 | 2.753 | 0.586 | 3.364 | 3.364 | 3.364 | 3.669 |
| WET\_RCON\_GOFF | Attack | 0 | 0 | 0 | 0 | 0 | 0 | 1.024 | 0 | 1.024 | 1.024 | 0 | 0.683 | 0.683 | 0.683 | 0.512 |
| Normal | 0 | 0 | 0 | 0 | 0 | 0 | 3.835 | 0 | 3.835 | 3.835 | 0 | 5.114 | 5.114 | 5.114 | 5.753 |
| WET\_RCON\_GON | Attack | 0.74 | 0.74 | 0.74 | 1.857 | 0.74 | 0.74 | 1.517 | 0.74 | 1.517 | 1.517 | 0.74 | 1.4 | 1.4 | 1.404 | 1.347 |
| Normal | 0.541 | 0.541 | 0.541 | 0.91 | 0.541 | 0.541 | 2.76 | 0.541 | 2.76 | 2.76 | 0.541 | 3.377 | 3.377 | 3.377 | 3.685 |
| WID\_RCOFF\_GOFF | Attack | 0.056 | 0.056 | 0.056 | 0.124 | 0.056 | 0.056 | 2.063 | 0.056 | 2.063 | 2.063 | 0.056 | 2.709 | 2.709 | 2.709 | 3.033 |
| Normal | 0.162 | 0.162 | 0.162 | 0.118 | 0.162 | 0.162 | 4.293 | 0.162 | 4.293 | 4.293 | 0.162 | 5.685 | 5.685 | 5.685 | 6.381 |
| WID\_RCOFF\_GON | Attack | 0.438 | 0.438 | 0.438 | 1.325 | 0.438 | 0.438 | 1.089 | 0.438 | 1.089 | 1.089 | 0.438 | 1.01 | 1.01 | 1.01 | 0.971 |
| Normal | 0.619 | 0.619 | 0.619 | 0.886 | 0.619 | 0.619 | 2.789 | 0.619 | 2.789 | 2.789 | 0.619 | 3.423 | 3.423 | 3.423 | 3.74 |
| WID\_RCON\_GOFF | Attack | 0.104 | 0.104 | 0.104 | 0.179 | 0.104 | 0.104 | 0.411 | 0.104 | 0.411 | 0.411 | 0.104 | 0.309 | 0.309 | 0.309 | 0.257 |
| Normal | 0.063 | 0.063 | 0.063 | 0.161 | 0.063 | 0.063 | 4.098 | 0.063 | 4.098 | 4.098 | 0.063 | 5.411 | 5.411 | 5.411 | 6.067 |
| WID\_RCON\_GON | Attack | 0.399 | 0.399 | 0.399 | 1.379 | 0.399 | 0.399 | 1.016 | 0.399 | 1.016 | 1.016 | 0.399 | 0.895 | 0.895 | 0.895 | 0.834 |
| Normal | 0.6 | 0.6 | 0.6 | 0.913 | 0.6 | 0.6 | 2.643 | 0.6 | 2.643 | 2.643 | 0.6 | 3.22 | 3.22 | 3.22 | 3.509 |

Table 12. The combined loss rate of GS in the attack scenarios

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Sub-Scenario Abbreviation | Mode | Index in Table 6 | | | | | | | | | | | | | | |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
| CID\_RCOFF\_GOFF | Attack | 0 | 0 | 0 | 0.124 | 0 | 0 | 1.092 | 0 | 1.092 | 1.092 | 0 | 1.673 | 1.673 | 1.673 | 2.06 |
| Normal | 0 | 0 | 0 | 0.117 | 0 | 0 | 1.48 | 0 | 1.48 | 1.48 | 0 | 2.297 | 2.297 | 2.297 | 2.842 |
| CID\_RCOFF\_GON | Attack | 0 | 0 | 0 | 1.311 | 0 | 0 | 20.076 | 0 | 20.076 | 20.076 | 0 | 31.335 | 31.335 | 31.335 | 38.842 |
| Normal | 0 | 0 | 0 | 0.895 | 0 | 0 | 1.649 | 0 | 1.649 | 1.649 | 0 | 2.101 | 2.101 | 2.101 | 2.402 |
| CID\_RCON\_GOFF | Attack | 0 | 0 | 0 | 0.075 | 0 | 0 | 0.551 | 0 | 0.551 | 0.551 | 0 | 0.413 | 0.413 | 0.413 | 0.33 |
| Normal | 0 | 0 | 0 | 0.068 | 0 | 0 | 1.843 | 0 | 1.843 | 1.843 | 0 | 2.73 | 2.73 | 2.73 | 3.262 |
| CID\_RCON\_GON | Attack | 0 | 0 | 0 | 1.406 | 0 | 0 | 1.127 | 0 | 1.127 | 1.127 | 0 | 0.845 | 0.845 | 0.845 | 0.676 |
| Normal | 0 | 0 | 0 | 0.761 | 0 | 0 | 1.618 | 0 | 1.618 | 1.618 | 0 | 2.047 | 2.047 | 2.047 | 2.304 |
| WCT\_RCOFF\_GOFF | Attack | 0 | 0 | 0 | 0.124 | 0 | 0 | 1.083 | 0 | 1.083 | 1.083 | 0 | 1.659 | 1.659 | 1.659 | 2.043 |
| Normal | 0 | 0 | 0 | 0.118 | 0 | 0 | 1.49 | 0 | 1.49 | 1.49 | 0 | 2.314 | 2.314 | 2.314 | 2.863 |
| WCT\_RCOFF\_GON | Attack | 0 | 0 | 0 | 1.34 | 0 | 0 | 1.101 | 0 | 1.101 | 1.101 | 0 | 0.958 | 0.958 | 0.958 | 0.862 |
| Normal | 0 | 0 | 0 | 0.918 | 0 | 0 | 1.643 | 0 | 1.643 | 1.643 | 0 | 2.077 | 2.077 | 2.077 | 2.367 |
| WCT\_RCON\_GOFF | Attack | 0 | 0 | 0 | 0.078 | 0 | 0 | 0.784 | 0 | 0.784 | 0.784 | 0 | 0.588 | 0.588 | 0.588 | 0.47 |
| Normal | 0 | 0 | 0 | 0.07 | 0 | 0 | 1.849 | 0 | 1.849 | 1.849 | 0 | 2.739 | 2.739 | 2.739 | 3.273 |
| WCT\_RCON\_GON | Attack | 0 | 0 | 0 | 1.28 | 0 | 0 | 0.997 | 0 | 0.997 | 0.997 | 0 | 0.826 | 0.826 | 0.826 | 0.713 |
| Normal | 0 | 0 | 0 | 0.916 | 0 | 0 | 1.638 | 0 | 1.638 | 1.638 | 0 | 2.071 | 2.071 | 2.071 | 2.36 |
| WET\_RCOFF\_GOFF | Attack | 0 | 0 | 0 | 0.131 | 0 | 0 | 0.545 | 0 | 0.545 | 0.545 | 0 | 0.436 | 0.436 | 0.436 | 0.363 |
| Normal | 0 | 0 | 0 | 0.123 | 0 | 0 | 1.478 | 0 | 1.478 | 1.478 | 0 | 2.291 | 2.291 | 2.291 | 2.833 |
| WET\_RCOFF\_GON | Attack | 0 | 0 | 0 | 1.333 | 0 | 0 | 1.113 | 0 | 1.113 | 1.113 | 0 | 0.98 | 0.98 | 0.98 | 0.892 |
| Normal | 0 | 0 | 0 | 0.921 | 0 | 0 | 1.681 | 0 | 1.681 | 1.681 | 0 | 2.137 | 2.137 | 2.137 | 2.441 |
| WET\_RCON\_GOFF | Attack | 0 | 0 | 0 | 0 | 0 | 0 | 2.977 | 0 | 2.977 | 2.977 | 0 | 1.984 | 1.984 | 1.984 | 1.488 |
| Normal | 0 | 0 | 0 | 0 | 0 | 0 | 2.822 | 0 | 2.822 | 2.822 | 0 | 3.763 | 3.763 | 3.763 | 4.233 |
| WET\_RCON\_GON | Attack | 0 | 0 | 0 | 1.857 | 0 | 0 | 1.529 | 0 | 1.529 | 1.529 | 0 | 1.332 | 1.332 | 1.332 | 1.201 |
| Normal | 0 | 0 | 0 | 0.91 | 0 | 0 | 0.749 | 0 | 0.749 | 0.749 | 0 | 0.653 | 0.653 | 0.653 | 0.589 |
| WID\_RCOFF\_GOFF | Attack | 0 | 0 | 0 | 0.124 | 0 | 0 | 1.087 | 0 | 1.087 | 1.087 | 0 | 1.664 | 1.664 | 1.664 | 2.049 |
| Normal | 0 | 0 | 0 | 0.118 | 0 | 0 | 1.537 | 0 | 1.537 | 1.537 | 0 | 2.389 | 2.389 | 2.389 | 2.956 |
| WID\_RCOFF\_GON | Attack | 0 | 0 | 0 | 1.325 | 0 | 0 | 1.097 | 0 | 1.097 | 1.097 | 0 | 0.961 | 0.961 | 0.961 | 0.87 |
| Normal | 0 | 0 | 0 | 0.886 | 0 | 0 | 1.785 | 0 | 1.785 | 1.785 | 0 | 2.324 | 2.324 | 2.324 | 2.683 |
| WID\_RCON\_GOFF | Attack | 0 | 0 | 0 | 0.179 | 0 | 0 | 0.482 | 0 | 0.482 | 0.482 | 0 | 0.361 | 0.361 | 0.361 | 0.289 |
| Normal | 0 | 0 | 0 | 0.161 | 0 | 0 | 1.887 | 0 | 1.887 | 1.887 | 0 | 2.75 | 2.75 | 2.75 | 3.268 |
| WID\_RCON\_GON | Attack | 0 | 0 | 0 | 1.379 | 0 | 0 | 1.206 | 0 | 1.206 | 1.206 | 0 | 1.103 | 1.103 | 1.103 | 1.034 |
| Normal | 0 | 0 | 0 | 0.913 | 0 | 0 | 1.652 | 0 | 1.652 | 1.652 | 0 | 2.095 | 2.095 | 2.095 | 2.391 |

The features are downsized using the feature downsizing technique proposed in this paper. Nonetheless, they cannot be the same as the original samples. In this paper, the loss of information from original features is called the "combined loss rate" in Tables 11 and 12. The "sampling resolution" in Tables 7 and 8 is used to calculate the combined loss rate of Tables 11 and 12. The instruction, cycle, and branch Perf STAT features have various combined loss rates in the CS, but the GS shows zero in the features. This is because the CS extracts three different Perf STAT data points, so the sizes of these features are different. However, the GS has the same Perf STAT feature size because only one GS exists in this research.

Table 13. The list of the symbols used in the pseudo-code

|  |  |  |  |
| --- | --- | --- | --- |
| Symbol | Explanation | symbol | Explanation |
|  | CS feature list |  | Sampling resolution list of a GS |
| [ ] | GS feature list |  | Minimum size among features |
|  | Perf STAT feature list on different CS |  | Minimum size among features |
|  | Perf STAT feature list on a GS | sum( ) | Function that adds all elements of a list |
| len( ) | A function that calculates the size of a feature |  | Temporal list for CS |
|  | Simulation time on different CS |  | Temporal list for GS |
|  | Simulation time on a GS |  | A combined loss rate of CS features |
|  | Sampling resolution list of different CS |  | A combined loss rate of GS features |

Table 13 shows the symbols referenced in the pseudo-code that calculates the combination loss rate on CS and GS.

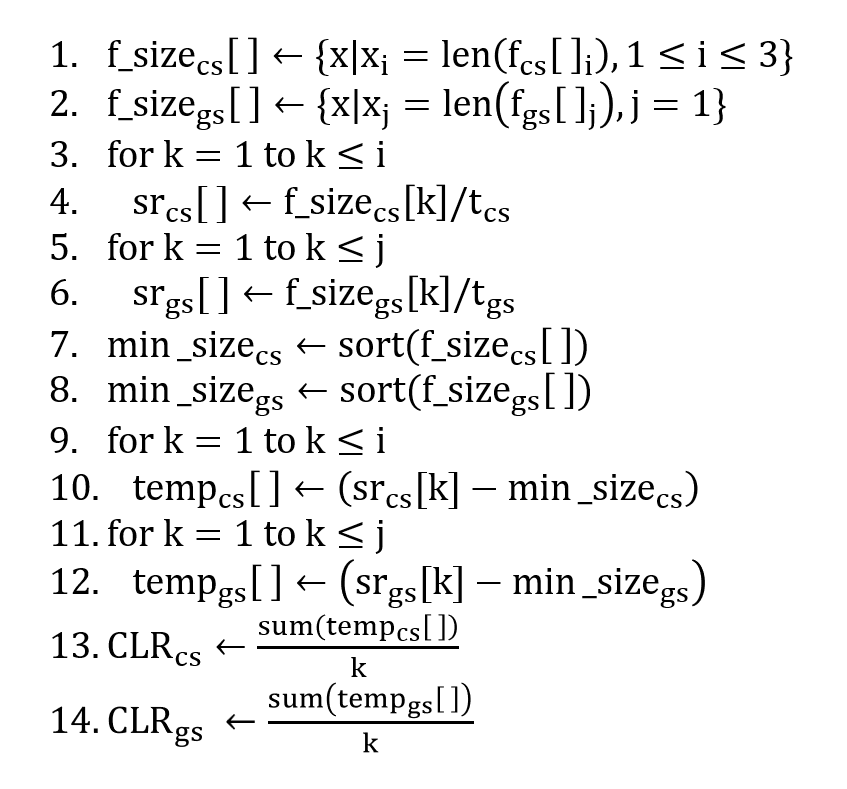


Figure 19. Pseudo code of the proposed calculation method on the combined loss rate

Figure 19 is a pseudo-code that calculates the information loss rate of original features that inevitably occurs in integrating features after downsizing them through the method in Figures 8 and 9. Perf STAT's instruction, cycle, branch, and Time Delta features are extracted from different CS and integrated separately into the types of those features. However, a separate feature integration process is unnecessary since only one GS exists. These instruction, branch, cycle, and Time Delta features are created and used as basic features. As shown in Table 6, these basic features are combined to create 15 Perf STAT and Time Delta feature combinations of CS and GS. The combined loss rates according to the feature combinations are listed in Tables 11 and 12.

### Perf TOP Features

The Perf TOP records the overheads of the Linux kernel processes loaded into the simulator concerning instruction, branch, and cycle on Perf STAT. In other words, one of the overheads is the percentage of resources consumed relative to Perf STAT's instructions, branches, and cycles in a particular kernel process.

Table 14. Counts in the Perf TOP measurement

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Category | CPU Clock | | | STD / AVG |
| 900 MHz | 1800 MHz | 2700 MHz |
| Cycle | 458295317907 | 451901542572 | 450139539513 | 0.008 |
| Branch | 42458598176 | 42245638417 | 42176076909 | 0.002 |
| Instruction | 156553532325 | 155190349191 | 154757185367 | 0.005 |

Table 14 results from Sysbench's CPU prime factorization operation measured with the Perf TOP. The CPU clocks are downclocked to 900, 1800, and 2700 MHz, respectively, and all experiments were done on the same Intel(R) Core(TM) i5-8265U. Ubuntu kernel version is 22.04.1 LTS, Perf version is 5.15.74, and Sysbench version is 1.0.2. The number of threads used in Sysbench is 8, and the maximum value of prime factorization for each thread is 10000000. The Perf STAT counts Sysbench based on cycle, branch, or instruction at 4 KHz intervals. STD / AVG is the standard deviation divided by the average of counted resources concerning the cycle, branch, and instruction. Since the differences of STD / AVG are very small, It is proved that the Perf STAT measurement value shows consistency without being affected by different CPU performances.

### Profiling System Overheads

Table 15. Comparison of the performance differences among the Perf TOP results

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Type | Sysbench Comparisons in Different CPU Clocks | | | Kernel Symbol Name |
| 900 MHz | 1800 MHz | 2700 MHz |
| Cycle | 0.07% | -0.04% | -0.05% | error\_entry |
| 0.03% | -0.02% | -0.02% | native\_write\_msr |
| 0.03% | -0.02% | -0.02% | irqentry\_exit\_to\_user\_mode |
| 0.01% | -0.01% | -0.01% | lapic\_next\_deadline |
| 0.01% | -0.01% | -0.01% | xhci\_irq |
| 0.02% | -0.01% | -0.01% | \_\_irqentry\_text\_end |
| 0.01% | 0.00% | 0.00% | ktime\_get |
| 0.01% | 0.00% | 0.00% | \_\_irq\_exit\_rcu |
| 0.01% | 0.00% | 0.00% | read\_tsc |
| 0.01% | 0.00% | 0.00% | native\_apic\_msr\_eoi\_write |
| Branch | 0.02% | -0.01% | -0.01% | psi\_group\_change |
| 0.01% | -0.01% | -0.01% | \_\_update\_load\_avg\_se |
| 0.01% | -0.01% | -0.01% | \_\_update\_load\_avg\_cfs\_rq |
| 0.01% | 0.00% | 0.00% | \_\_hrtimer\_run\_queues |
| 0.01% | 0.00% | 0.00% | update\_curr |
| 0.01% | 0.00% | 0.00% | task\_tick\_fair |
| 0.01% | 0.00% | -0.01% | update\_load\_avg |
| 0.00% | 0.00% | 0.00% | timerqueue\_add |
| 0.01% | 0.00% | 0.00% | \_\_hrtimer\_next\_event\_base |
| 0.00% | 0.00% | 0.00% | \_\_calc\_delta |
| Instruction | 0.01% | -0.01% | -0.01% | psi\_group\_change |
| 0.01% | 0.00% | -0.01% | \_raw\_spin\_lock |
| 0.05% | 0.00% | -0.03% | \_\_update\_load\_avg\_se |
| 0.01% | 0.00% | 0.00% | \_\_hrtimer\_next\_event\_base |
| 0.01% | 0.00% | -0.01% | task\_tick\_fair |
| 0.01% | 0.00% | 0.00% | scheduler\_tick |
| 0.01% | 0.00% | 0.00% | rcu\_sched\_clock\_irq |
| 0.01% | 0.00% | 0.00% | native\_sched\_clock |
| 0.02% | 0.00% | -0.01% | update\_load\_avg |
| 0.00% | 0.00% | 0.00% | arch\_scale\_freq\_tick |

Table 15 compares the Perf Record [40] results from Sysbench in Table 14. The Perf Record data collected in the 900 MHz CPU down-clock setting environment shows the difference comparison between the Perf Record values ​​of 1800 MHz and 2700 MHz. Among many kernel symbols, the top 10 overhead kernel symbols were targeted. Since the difference is between 0.00% and 0.07%, there is almost no measurement difference depending on the CPU clock. The Perf Record shows statistical values ​​about the overheads of symbols during an entire profiling session based on individual Perf TOP measurements. There is almost no difference in the Perf Record comparison in Table 14. In this regard, it is also proved that the difference in the overhead of symbols does not occur in the Perf TOP measurements on different CPU performances.

## Feature Transformation

The main features of Perf TOP consist of the 16 DDoS attack scenarios and 16 normal EV authentication scenarios, as shown in Table 2. The features are divided into the CS and GS under these scenarios, which are collected through the simulator [1]. These main features are composed of many symbols. This symbol means the name of a function executed in a process in the Linux kernel [41]. Only one GS is used in this study, but multiple CSs exist. Therefore, symbol features extracted from each scenario must be common to the different CSs. This is because the decision boundary of the ML model can be designed to reflect the characteristics of all the CS, not a specific CS.

Table 16. Unique and commonly found symbols on different CS under the CID\_RCOFF\_GOFF attack scenario in Table 2

|  |  |  |  |
| --- | --- | --- | --- |
| Type | Branch | Cycle | Instruction |
| Attack | dequeue\_task\_fair | dequeue\_task\_fair | x86\_get\_event\_constraints |
| update\_load\_avg | update\_load\_avg | kmem\_cache\_alloc\_node |
|  | | |
| perf\_event\_groups\_first | perf\_event\_groups\_first | perf\_swevent\_add |
| iterate\_groups | iterate\_groups | kfree |
| Normal | kmem\_cache\_alloc\_node | perf\_event\_alloc | event\_sched\_in |
| visit\_groups\_merge.constprop.0.is | x86\_pmu\_event\_init |
|  | inherit\_event.constprop.0 |
| perf\_event\_groups\_insert | intel\_pmu\_enable\_all |
| perf\_event\_update\_time |

Table 16 lists common and unique symbols from various CS under the CID\_RCOFF\_GOFF scenario in Table 2. The symbols for branch, cycle, and instruction features were extracted. The other unique and common symbols are extracted for each attack scenario in Table 2. In other words, 16 symbol lists, such as Table 16, are created.

### Feature Size Synchronization by Down Sampling

Table 17. Basic Perf TOP CS features under the CID\_RCOFF\_GOFF attack scenario

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Type | Mode | Symbol Name | CS ID | Sampling Count (SC) | Sampling Resolution (SR) |
| Branch | Attack | dequeue\_task\_fair | 2-39-139-28 | 59 | 0.154 |
| 2-39-89-25 | 5 | 0.013 |
| 2-39-131-30 | 12 | 0.031 |
| update\_load\_avg | 2-39-139-28 | 48 | 0.125 |
| 2-39-89-25 | 65 | 0.17 |
| 2-39-131-30 | 65 | 0.17 |
|  | | | |
| perf\_event\_groups\_first | 2-39-139-28 | 14 | 0.036 |
| 2-39-89-25 | 83 | 0.217 |
| 2-39-131-30 | 89 | 0.232 |
| iterate\_groups | 2-39-139-28 | 86 | 0.225 |
| 2-39-89-25 | 63 | 0.164 |
| 2-39-131-30 | 66 | 0.172 |
| Normal | kmem\_cache\_alloc\_node | 2-39-139-28 | 36 | 0.089 |
| 2-39-89-25 | 67 | 0.165 |
| 2-39-131-30 | 52 | 0.128 |
| visit\_groups\_merge.constprop.0.is | 2-39-139-28 | 20 | 0.049 |
| 2-39-89-25 | 124 | 0.306 |
| 2-39-131-30 | 45 | 0.111 |
|  | | | |
| perf\_event\_groups\_insert | 2-39-139-28 | 91 | 0.225 |
| 2-39-89-25 | 64 | 0.158 |
| 2-39-131-30 | 101 | 0.249 |
| perf\_event\_update\_time | 2-39-139-28 | 43 | 0.106 |
| 2-39-89-25 | 69 | 0.17 |
| 2-39-131-30 | 32 | 0.079 |
| Cycle | Attack | dequeue\_task\_fair | 2-39-139-28 | 7 | 0.018 |
| 2-39-89-25 | 10 | 0.026 |
| 2-39-131-30 | 103 | 0.269 |
| update\_load\_avg | 2-39-139-28 | 32 | 0.083 |
| 2-39-89-25 | 47 | 0.122 |
| 2-39-131-30 | 73 | 0.191 |
|  | | | |
| perf\_event\_groups\_first | 2-39-139-28 | 118 | 0.308 |
| 2-39-89-25 | 14 | 0.036 |
| 2-39-131-30 | 16 | 0.041 |
| iterate\_groups | 2-39-139-28 | 42 | 0.109 |
| 2-39-89-25 | 8 | 0.02 |
| 2-39-131-30 | 26 | 0.068 |
| Normal | perf\_event\_alloc | 2-39-139-28 | 88 | 0.217 |
| 2-39-89-25 | 12 | 0.029 |
| 2-39-131-30 | 114 | 0.281 |
| Instruction | Attack | x86\_get\_event\_constraints | 2-39-139-28 | 122 | 0319 |
| 2-39-89-25 | 106 | 0.277 |
| 2-39-131-30 | 77 | 0.201 |
| kmem\_cache\_alloc\_node | 2-39-139-28 | 129 | 0.337 |
| 2-39-89-25 | 197 | 0.515 |
| 2-39-131-30 | 225 | 0.588 |
|  | | | |
| perf\_swevent\_add | 2-39-139-28 | 34 | 0.088 |
| 2-39-89-25 | 33 | 0.086 |
| 2-39-131-30 | 56 | 0.146 |
| kfree | 2-39-139-28 | 288 | 0.753 |
| 2-39-89-25 | 271 | 0.709 |
| 2-39-131-30 | 273 | 0.714 |
| Normal | event\_sched\_in | 2-39-139-28 | 129 | 0.319 |
| 2-39-89-25 | 12 | 0.029 |
| 2-39-131-30 | 177 | 0.437 |
| x86\_pmu\_event\_init | 2-39-139-28 | 70 | 0.173 |
| 2-39-89-25 | 84 | 0.207 |
| 2-39-131-30 | 44 | 0.108 |
| \_raw\_spin\_lock\_irqsave | 2-39-139-28 | 56 | 0.138 |
| 2-39-89-25 | 86 | 0.212 |
| 2-39-131-30 | 50 | 0.123 |
| intel\_pmu\_enable\_all | 2-39-139-28 | 1 | 0.002 |
| 2-39-89-25 | 1 | 0.002 |
| 2-39-131-30 | 1 | 0.002 |

In Table 17, "Sampling Count" means the number of measured overhead data of a symbol. The PMU records the overhead by measuring Perf TOP perf 1 second with a resolution of 4 KHz. The number of these data is "Sampling Count (SC)." "Sampling Resolution (SR)" is calculated as follows.

Since the SR increases as the amount of data collected during a specific time ST increases, the higher the SR of a symbol, the better as a robust feature. In other words, a high SR value indicates that the symbol has strong feature characteristics on activities related to the EV charging infrastructure.

Table 18. Basic Perf TOP GS features under the CID\_RCOFF\_GOFF attack scenario

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Type | Mode | Symbol Name | Sampling Count (SC) | Sampling Resolution (SR) |
| Branch | Attack | tcp\_recvmsg | 4 | 0.01 |
| security\_sock\_rcv\_skb | 14 | 0.036 |
|  | | |
| \_\_sys\_sendto | 25 | 0.065 |
| dst\_release | 11 | 0.028 |
| Normal | security\_sock\_rcv\_skb | 40 | 0.098 |
| pick\_next\_task | 1 | 0.002 |
|  | | |
| \_\_update\_load\_avg\_cfs\_rq | 110 | 0.272 |
| acct\_account\_cputime | 12 | 0.029 |
| Cycle | Attack | tcp\_recvmsg | 1 | 0.002 |
| security\_sock\_rcv\_skb | 6 | 0.015 |
|  | | |
| \_\_sys\_sendto | 14 | 0.036 |
| dst\_release | 7 | 0.018 |
| Normal | tcp\_recvmsg | 12 | 0.029 |
| security\_sock\_rcv\_skb | 4 | 0.009 |
|  | | |
| \_\_update\_load\_avg\_cfs\_rq | 85 | 0.21 |
| dst\_release | 7 | 0.017 |
| Instruction | Attack | tcp\_recvmsg | 14 | 0.036 |
| security\_sock\_rcv\_skb | 1 | 0.002 |
|  | | |
| \_\_sys\_sendto | 4 | 0.01 |
| dst\_release | 4 | 0.01 |
| Normal | pick\_next\_task | 18 | 0.044 |
| \_\_x64\_sys\_poll | 32 | 0.079 |
|  | | |
| \_\_update\_load\_avg\_cfs\_rq | 85 | 0.21 |
| ip\_rcv\_core | 16 | 0.039 |

Tables 17 and 18 show basic features with symbol overhead information for the CS and GS. In Table 18, since only one GS is used in this study, there is no need for the common and unique feature classification task of Table 16. Since there are 16 scenarios in Table 2, for tables 17 and 18, 32 tables are created, each with 16 tables.

Table 19. Average Sampling Resolution (ASR) and ASR Difference (ASRD) of CS features under the CID\_RCOFF\_GOFF attack scenario

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Type | Mode | Symbol Name | ASR | ASRD |
| Branch | Attack | dequeue\_task\_fair | 0.066 | 0.053 |
| update\_load\_avg | 0.155 | 0.029 |
|  | | |
| perf\_event\_groups\_first | 0.162 | 0.125 |
| iterate\_groups | 0.187 | 0.022 |
| Normal | kmem\_cache\_alloc\_node | 0.127 | 0.038 |
| visit\_groups\_merge.constprop.0.is | 0.155 | 0.106 |
|  | | |
| perf\_event\_groups\_insert | 0.211 | 0.052 |
| perf\_event\_update\_time | 0.118 | 0.039 |
| Cycle | Attack | dequeue\_task\_fair | 0.106 | 0.086 |
| update\_load\_avg | 0.132 | 0.048 |
|  | | |
| perf\_event\_groups\_first | 0.129 | 0.092 |
| iterate\_groups | 0.066 | 0.045 |
| Normal | perf\_event\_alloc | 0.176 | 0.146 |
| Instruction | Attack | x86\_get\_event\_constraints | 0.266 | 0.064 |
| kmem\_cache\_alloc\_node | 0.48 | 0.143 |
|  | | |
| perf\_swevent\_add | 0.107 | 0.02 |
| kfree | 0.725 | 0.016 |
| Normal | event\_sched\_in | 0.262 | 0.232 |
| x86\_pmu\_event\_init | 0.163 | 0.054 |
| inherit\_event.constprop.0 | 0.248 | 0.042 |
| intel\_pmu\_enable\_all | 0.002 | 0.0 |

Table 19 shows that the same types of symbols in Table 17 are extracted from all the CS and integrated. Since the SC of each symbol in Table 17 differs, an imbalance in feature size occurs in integrating features. ASR means the average of sampling resolutions generated after integrating identical symbols extracted from each CS. In this study, downsizing is performed based on the smallest size feature in the feature integration process. Therefore, based on the ASR of the smallest symbol to be merged, the difference between the ASRs of other symbols to be merged is calculated. The average of these ASR differences is called the ASRD. ASR and ASRD are as follows.

Based on the ASRD value, the information loss rate can be calculated when combining different symbols.

Table 20. ASR and ASRD of GS features under the CID\_RCOFF\_GOFF attack scenario

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Type | Mode | Symbol Name | ASR | ASRD |
| Branch | Attack | tcp\_recvmsg | 0.01 | 0.0 |
| security\_sock\_rcv\_skb | 0.036 | 0.0 |
|  | | |
| \_\_sys\_sendto | 0.065 | 0.0 |
| dst\_release | 0.028 | 0.0 |
| Normal | security\_sock\_rcv\_skb | 0.098 | 0.0 |
| pick\_next\_task | 0.002 | 0.0 |
|  | | |
| \_\_update\_load\_avg\_cfs\_rq | 0.272 | 0.0 |
| acct\_account\_cputime | 0.029 | 0.0 |
| Cycle | Attack | tcp\_recvmsg | 0.002 | 0.0 |
| security\_sock\_rcv\_skb | 0.015 | 0.0 |
|  | | |
| \_\_sys\_sendto | 0.036 | 0.0 |
| dst\_release | 0.018 | 0.0 |
| Normal | tcp\_recvmsg | 0.029 | 0.0 |
| security\_sock\_rcv\_skb | 0.009 | 0..0 |
|  | | |
| \_\_update\_load\_avg\_cfs\_rq | 0.21 | 0.0 |
| dst\_release | 0.017 | 0.0 |
| Instruction | Attack | tcp\_recvmsg | 0.036 | 0.0 |
| security\_sock\_rcv\_skb | 0.002 | 0.0 |
|  | | |
| \_\_sys\_sendto | 0.01 | 0.0 |
| dst\_release | 0.01 | 0.0 |
| Normal | pick\_next\_task | 0.044 | 0.0 |
| \_\_x64\_sys\_poll | 0.079 | 0.0 |
|  | | |
| \_\_update\_load\_avg\_cfs\_rq | 0.21 | 0.0 |
| ip\_rcv\_core | 0.039 | 0.0 |

Table 20 lists ASR and ASRD values ​​for the symbols of the GS. These ASR values are the same as the SR of the GS in Table 18, and all ASRD values are 0. This is because features of the same type cannot be duplicated in a different GS. As mentioned earlier, we have only one GS in this study. Since there are 16 scenarios in Table 2, for tables 19 and 20, 32 tables are created, each with 16 tables.

## Feature Creation

### Combining Different Features

Table 21. CS Perf TOP symbol combination under the CID\_RCOFF\_GOFF attack scenario

(N/A: Not Available, MC: Minimum-sampling Count)

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Mode  Type 1, Type 2, Symbol | | | Attack | | | Normal | | |
| MC | ASR | ASRD | MC | ASR | ASRD |
| Branch | Common | ctx\_sched\_in | 50 | 0.158 | 0.027 | 69 | 0.221 | 0.051 |
| \_\_update\_load\_avg\_se | 53 | 0.226 | 0.088 | 20 | 0.132 | 0.083 |
|  | | | | | | |
| kmem\_cache\_alloc\_trace | 123 | 0.386 | 0.064 | 24 | 0.169 | 0.11 |
| update\_load\_avg | 48 | 0.155 | 0.029 | 64 | 0.202 | 0.044 |
| Exclusive | memcg\_slab\_free\_hook | 84 | 0.33 | 0.11 | 0 | N/A | N/A |
| update\_rq\_clock | 9 | 0.095 | 0.072 | 0 | N/A | N/A |
|  | | | | | | |
| perf\_try\_init\_event | 0 | N/A | N/A | 45 | 0.208 | 0.097 |
| perf\_event\_update\_time | 0 | N/A | N/A | 32 | 0.118 | 0.039 |
| All | ctx\_sched\_in | 50 | 0.158 | 0.027 | 69 | 0.221 | 0.051 |
| \_\_update\_load\_avg\_se | 53 | 0.226 | 0.088 | 20 | 0.132 | 0.083 |
|  | | | | | | |
| perf\_try\_init\_event | 0 | N/A | N/A | 45 | 0.208 | 0.097 |
| perf\_event\_update\_time | 0 | N/A | N/A | 32 | 0.118 | 0.039 |
| Cycle | Common | perf\_event\_alloc | 291 | 0.805 | 0.044 | 12 | 0.176 | 0.146 |
| Exclusive | native\_write\_msr | 1 | 0.103 | 0.101 | 0 | N/A | N/A |
| memcg\_slab\_free\_hook | 9 | 0.112 | 0.088 | 0 | N/A | N/A |
|  | | | | | | |
| list\_add\_event | 19 | 0.11 | 0.061 | 0 | N/A | N/A |
| \_\_update\_load\_avg\_cfs\_rq | 5 | 0.059 | 0.046 | 0 | N/A | N/A |
| All | perf\_event\_alloc | 291 | 0.805 | 0.044 | 12 | 0.176 | 0.146 |
| native\_write\_msr | 1 | 0.103 | 0.101 | 0 | N/A | N/A |
|  | | | | | | |
| list\_add\_event | 19 | 0.11 | 0.061 | 0 | N/A | N/A |
| \_\_update\_load\_avg\_cfs\_rq | 5 | 0.059 | 0.046 | 0 | N/A | N/A |
| Instruction | Common | x86\_pmu\_event\_init | 73 | 0.229 | 0.038 | 44 | 0.163 | 0.054 |
| psi\_group\_change | 255 | 0.762 | 0.095 | 84 | 0.323 | 0.115 |
|  | | | | | | |
| \_raw\_spin\_lock\_irqsave | 42 | 0.215 | 0.105 | 50 | 0.158 | 0.034 |
| inherit\_event.constprop.0 | 136 | 0.412 | 0.056 | 83 | 0.248 | 0.042 |
| Exclusive | intel\_pmu\_hw\_config.part.0 | 4 | 0.111 | 0.101 | 0 | N/A | N/A |
| memcg\_slab\_free\_hook | 57 | 0.375 | 0.226 | 0 | N/A | N/A |
|  | | | | | | |
| calc\_timer\_values | 19 | 0.114 | 0.064 | 0 | N/A | N/A |
| intel\_pmu\_enable\_all | 0 | N/A | N/A | 1 | 0.002 | 0 |
| All | x86\_pmu\_event\_init | 70 | 0.268 | 0.085 | 0 | N/A | N/A |
| psi\_group\_change | 65 | 0.42 | 0.25 | 0 | N/A | N/A |
|  | | | | | | |
| calc\_timer\_values | 19 | 0.114 | 0.064 | 0 | N/A | N/A |
| intel\_pmu\_enable\_all | 0 | N/A | N/A | 1 | 0.002 | 0 |

Table 22. GS Perf TOP symbol combination under the CID\_RCOFF\_GOFF attack scenario

**(N/A: Not Available, MC: Minimum-sampling Count)**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Mode  Type 1, Type 2, Symbol | | | Attack | | | Normal | | |
| MC | ASR | ASRD | MC | ASR | ASRD |
| Branch | Common | security\_sock\_rcv\_skb | 14 | 0.036 | 0 | 40 | 0.098 | 0 |
| pick\_next\_task | 3 | 0.007 | 0 | 1 | 0.002 | 0 |
|  | | | | | | |
| \_\_update\_load\_avg\_cfs\_rq | 80 | 0.209 | 0 | 110 | 0.272 | 0 |
| ip\_rcv\_core | 60 | 0.156 | 0 | 17 | 0.042 | 0 |
| Exclusive | tcp\_recvmsg | 4 | 0.01 | 0 | 0 | N/A | N/A |
| \_raw\_spin\_unlock\_bh | 3 | 0.007 | 0 | 0 | N/A | N/A |
|  | | | | | | |
| enqueue\_hrtimer | 0 | N/A | N/A | 6 | 0.014 | 0 |
| do\_vfs\_ioctl | 0 | N/A | N/A | 15 | 0.037 | 0 |
| All | security\_sock\_rcv\_skb | 6 | 0.015 | 0 | 4 | 0.009 | 0 |
| pick\_next\_task | 8 | 0.02 | 0 | 36 | 0.089 | 0 |
|  | | | | | | |
| enqueue\_hrtimer | 0 | N/A | N/A | 6 | 0.014 | 0 |
| do\_vfs\_ioctl | 0 | N/A | N/A | 15 | 0.037 | 0 |
| Cycle | Common | tcp\_recvmsg | 1 | 0.002 | 0 | 12 | 0.029 | 0 |
| security\_sock\_rcv\_skb | 6 | 0.015 | 0 | 4 | 0.009 | 0 |
|  | | | | | | |
| \_\_update\_load\_avg\_cfs\_rq | 23 | 0.06 | 0 | 85 | 0.21 | 0 |
| dst\_release | 7 | 0.018 | 0 | 7 | 0.017 | 0 |
| Exclusive | attach\_entity\_load\_avg | 2 | 0.005 | 0 | 0 | N/A | N/A |
| \_raw\_spin\_unlock\_bh | 1 | 0.002 | 0 | 0 | N/A | N/A |
|  | | | | | | |
| fput | 0 | N/A | N/A | 2 | 0.004 | 0 |
| enqueue\_hrtimer | 0 | N/A | N/A | 3 | 0.007 | 0 |
| All | tcp\_recvmsg | 1 | 0.007 | 0 | 18 | 0.044 | 0 |
| security\_sock\_rcv\_skb | 1 | 0.002 | 0 | 0 | N/A | N/A |
|  | | | | | | |
| fput | 0 | N/A | N/A | 2 | 0.004 | 0 |
| enqueue\_hrtimer | 0 | N/A | N/A | 3 | 0.007 | 0 |
| Instruction | Common | pick\_next\_task | 3 | 0.007 | 0 | 18 | 0.044 | 0 |
| \_\_update\_load\_avg\_se | 82 | 0.214 | 0 | 149 | 0.368 | 0 |
|  | | | | | | |
| \_\_update\_load\_avg\_cfs\_rq | 104 | 0.272 | 0 | 85 | 0.21 | 0 |
| ip\_rcv\_core | 49 | 0.128 | 0 | 16 | 0.039 | 0 |
| Exclusive | tcp\_recvmsg | 14 | 0.036 | 0 | 0 | N/A | N/A |
| security\_sock\_rcv\_skb | 1 | 0.002 | 0 | 0 | N/A | N/A |
|  | | | | | | |
| restore\_fpregs\_from\_fpstate | 0 | N/A | N/A | 36 | 0.089 | 0 |
| do\_vfs\_ioctl | 0 | N/A | N/A | 33 | 0.081 | 0 |
| All | pick\_next\_task | 3 | 0.007 | 0 | 18 | 0.044 | 0 |
| \_\_update\_load\_avg\_se | 82 | 0.214 | 0 | 149 | 0.368 | 0 |
|  | | | | | | |
| restore\_fpregs\_from\_fpstate | 0 | N/A | N/A | 36 | 0.089 | 0 |
| do\_vfs\_ioctl | 0 | N/A | N/A | 33 | 0.081 | 0 |

Tables 21 and 22 show the basic feature combinations of Perf TOP of CS and GS in the CID\_RCOFF\_GOFF scenario of Table 2. The "Common" category in "Type 2" classifies symbols found simultaneously in "Attack" and "Normal." "Exclusive" classifies symbols found only in either "Attack" or "Normal." "All" is the sum of the symbols of "Common" and "Exclusive." "Attack" means DDoS attack, and "Normal" means normal EV authentication. For the symbols in the "Exclusive" category, MC and ASRD values ​​of 0 and N/A mean that the PMU did not measure the symbols at "Attack" or "Normal." MC means the size of the smallest symbol as a feature when combining different-sized symbols but identical. As mentioned earlier, since there are three CS in this study, the CS features to be combined are reduced to the smallest feature size during the feature combination process. Therefore, the MC value of CS is variable. However, since only one GS exists, its MC value equals a single feature size. The following operation classifies the symbols of the type 2 category.

and are lists created by referring to the "Attack" and "Normal" modes in Tables 19 and 20. A dummy value -1 will be padded into symbols with MC and ASRD of 0 and N/A in the "Exclusive" category. The padding data size is a valid MC value greater than 0 in "Attack" or "Normal" in the same symbol. 16 Tables for each 21 and 22 are created according to the 16 attack scenarios in Table 2, respectively.

Table 23. CS Perf Top feature combinations under the CID\_RCOFF\_GOFF attack scenario

|  |  |  |  |
| --- | --- | --- | --- |
| Type 1 | Type 2 | Set Size | Symbol Set |
| Branch | Common | 1 | {psi\_group\_change}, , {kmem\_cache\_alloc\_trace} |
| 2 | {psi\_group\_change, perf\_event\_groups\_insert}, , {merge\_sched\_in, kmem\_cache\_alloc\_trace} |
| 3 | {psi\_group\_change, perf\_event\_groups\_insert, event\_sched\_in}, , {event\_sched\_in, merge\_sched\_in, kmem\_cache\_alloc\_trace} |
| 4 | {psi\_group\_change, perf\_event\_groups\_insert, event\_sched\_in, merge\_sched\_in}, , {perf\_event\_groups\_insert, event\_sched\_in, merge\_sched\_in, kmem\_cache\_alloc\_trace} |
| 5 | {psi\_group\_change, perf\_event\_groups\_insert, event\_sched\_in, merge\_sched\_in, kmem\_cache\_alloc\_trace} |
| Exclusive | 1 | {kfree}, , {kmem\_cache\_alloc\_node\_trace} |
| 2 | {kfree, inherit\_event.constprop.0}, , {perf\_event\_alloc, kmem\_cache\_alloc\_node\_trace} |
| 3 | {kfree, inherit\_event.constprop.0, rb\_next}, , {rb\_next, perf\_event\_alloc, kmem\_cache\_alloc\_node\_trace} |
| 4 | {kfree, inherit\_event.constprop.0, rb\_next, perf\_event\_alloc}, , {inherit\_event, rb\_next, perf\_event\_alloc, kmem\_cache\_alloc\_node\_trace} |
| 5 | {kfree, inherit\_event.constprop.0, rb\_next, perf\_event\_alloc, kmem\_cache\_alloc\_node\_trace} |
| All | 1 | {kfree}, , {rb\_next} |
| 2 | {kfree, psi\_group\_change}, , {perf\_event\_groups\_insert, rb\_next} |
| 3 | {kfree, psi\_group\_change, inherit\_event.constprop.0}, , {inherit\_event.constprop.0, perf\_event\_groups\_insert, rb\_next} |
| 4 | {kfree, psi\_group\_change, inherit\_event.constprop.0, perf\_event\_groups\_insert}, , {psi\_group\_change, inherit\_event.constprop.0, perf\_event\_groups\_insert, rb\_next} |
| 5 | {kfree, psi\_group\_change, inherit\_event.constprop.0, perf\_event\_groups\_insert, rb\_next} |
| Cycle | Common | 1 | {perf\_event\_alloc} |
| Exclusive | 1 | {memset\_erms}, , {psi\_group\_change} |
| 2 | {memset\_erms, rb\_next}, , {kfree, psi\_group\_change} |
| 3 | {memset\_erms, rb\_next, inherit\_event.constprop.0}, , {inherit\_event.constprop.0, kfree, psi\_group\_change} |
| 4 | {memset\_erms, rb\_next, inherit\_event.constprop.0, kfree}, , {rb\_next, inherit\_event.constprop.0, kfree, psi\_group\_change} |
| 5 | {memset\_erms, rb\_next, inherit\_event.constprop.0, kfree, psi\_group\_change} |
| All | 1 | {memset\_erms}, , {kfree} |
| 2 | {memset\_erms, rb\_next}, , {inherit\_event.constprop.0, kfree} |
| 3 | {memset\_erms, rb\_next, perf\_event\_alloc}, , {perf\_event\_alloc, inherit\_event.constprop.0, kfree} |
| 4 | {memset\_erms, rb\_next, perf\_event\_alloc, inherit\_event.constprop.0}, , {rb\_next, perf\_event\_alloc, inherit\_event.constprop.0, kfree} |
| 5 | {memset\_erms, rb\_next, perf\_event\_alloc, inherit\_event.constprop.0, kfree} |
| Instruction | Common | 1 | {psi\_group\_change}, , {x86\_pmu\_event\_init} |
| 2 | {psi\_group\_change, event\_sched\_in}, , {native\_sched\_clock, x86\_pmu\_event\_init} |
| 3 | {psi\_group\_change, event\_sched\_in, inherit\_event.constprop.0}, , {inherit\_event.constprop.0, native\_sched\_clock, x86\_pmu\_event\_init} |
| 4 | {psi\_group\_change, event\_sched\_in, inherit\_event.constprop.0, native\_sched\_clock}, , {event\_sched\_in , inherit\_event.constprop.0, inherit\_event.constprop.0, native\_sched\_clock, x86\_pmu\_event\_init} |
| 5 | {psi\_group\_change, event\_sched\_in, inherit\_event.constprop.0, native\_sched\_clock, x86\_pmu\_event\_init} |
| Exclusive | 1 | {kfree}, , {kmem\_cache\_alloc\_node\_trace} |
| 2 | {kfree, perf\_event\_alloc}, , {kmem\_cache\_alloc\_node , kmem\_cache\_alloc\_node\_trace} |
| 3 | {kfree, perf\_event\_alloc, merge\_sched\_in}, , {merge\_sched\_in, kmem\_cache\_alloc\_node, kmem\_cache\_alloc\_node\_trace} |
| 4 | {kfree, perf\_event\_alloc, merge\_sched\_in, kmem\_cache\_alloc\_node}, , {perf\_event\_alloc, merge\_sched\_in, kmem\_cache\_alloc\_node, kmem\_cache\_alloc\_node\_trace} |
| 5 | {kfree, perf\_event\_alloc, merge\_sched\_in, kmem\_cache\_alloc\_node, kmem\_cache\_alloc\_node\_trace} |
| All | 1 | {kfree}, , {perf\_event\_alloc} |
| 2 | {kfree, perf\_event\_alloc}, , {merge\_sched\_in , kmem\_cache\_alloc\_node} |
| 3 | {kfree, perf\_event\_alloc, psi\_group\_change}, , {psi\_group\_change, merge\_sched\_in, kmem\_cache\_alloc\_node} |
| 4 | {kfree, perf\_event\_alloc, psi\_group\_change, merge\_sched\_in}, , {perf\_event\_alloc ,psi\_group\_change, merge\_sched\_in, kmem\_cache\_alloc\_node} |
| 5 | {kfree, perf\_event\_alloc, merge\_sched\_in, kmem\_cache\_alloc\_node} |

Table 24. GS Perf Top feature combinations under the CID\_RCOFF\_GOFF attack scenario

|  |  |  |  |
| --- | --- | --- | --- |
| Type 1 | Type 2 | Set Size | Symbol Set |
| Branch | Common | 1 | {psi\_group\_change}, ,{rb\_next} |
| 2 | {psi\_group\_change, merge\_sched\_in}, ,{ visit\_groups\_merge.constprop.0.is, rb\_next} |
| 3 | {psi\_group\_change, merge\_sched\_in, event\_sched\_in}, ,{event\_sched\_in, visit\_groups\_merge.constprop.0.is, rb\_next} |
| 4 | {psi\_group\_change, merge\_sched\_in, event\_sched\_in, visit\_groups\_merge.constprop.0.is}, ,{merge\_sched\_in, event\_sched\_in, visit\_groups\_merge.constprop.0.is, rb\_next} |
| 5 | {psi\_group\_change, merge\_sched\_in, event\_sched\_in, visit\_groups\_merge.constprop.0.is, rb\_next} |
| Exclusive | 1 | {\_\_cgroup\_bpf\_run\_filter\_skb}, ,{skb\_release\_data} |
| 2 | {\_\_cgroup\_bpf\_run\_filter\_skb, timerqueue\_add}, ,{ tcp\_write\_xmit, skb\_release\_data} |
| 3 | {\_\_cgroup\_bpf\_run\_filter\_skb, timerqueue\_add, kmem\_cache\_free}, ,{kmem\_cache\_free, tcp\_write\_xmit, skb\_release\_data} |
| 4 | {\_\_cgroup\_bpf\_run\_filter\_skb, timerqueue\_add, kmem\_cache\_free, tcp\_write\_xmit}, ,{timerqueue\_add, kmem\_cache\_free, tcp\_write\_xmit, skb\_release\_data} |
| 5 | {\_\_cgroup\_bpf\_run\_filter\_skb, timerqueue\_add, kmem\_cache\_free, tcp\_write\_xmit, skb\_release\_data} |
| All | 1 | {psi\_group\_change}, ,{rb\_next} |
| 2 | {psi\_group\_change, merge\_sched\_in}, ,{ visit\_groups\_merge.constprop.0.is, rb\_next} |
| 3 | {psi\_group\_change, merge\_sched\_in, event\_sched\_in}, ,{ event\_sched\_in, visit\_groups\_merge.constprop.0.is, rb\_next} |
| 4 | {psi\_group\_change, merge\_sched\_in, event\_sched\_in, visit\_groups\_merge.constprop.0.is}, ,{merge\_sched\_in, event\_sched\_in, visit\_groups\_merge.constprop.0.is, rb\_next} |
| 5 | {psi\_group\_change, merge\_sched\_in, event\_sched\_in, visit\_groups\_merge.constprop.0.is, rb\_next} |
| Cycle | Common | 1 | {psi\_group\_change}, ,{perf\_event\_groups\_first} |
| 2 | {psi\_group\_change, syscall\_exit\_to\_user\_mode}, ,{ entry\_SYSCALL\_64\_after\_hwframe, perf\_event\_groups\_first} |
| 3 | {psi\_group\_change, syscall\_exit\_to\_user\_mode, perf\_event\_update\_userpage}, ,{perf\_event\_update\_userpage, entry\_SYSCALL\_64\_after\_hwframe, perf\_event\_groups\_first} |
| 4 | {psi\_group\_change, syscall\_exit\_to\_user\_mode, perf\_event\_update\_userpage, entry\_SYSCALL\_64\_after\_hwframe}, ,{ syscall\_exit\_to\_user\_mode, perf\_event\_update\_userpage, entry\_SYSCALL\_64\_after\_hwframe, perf\_event\_groups\_first} |
| 5 | {psi\_group\_change, syscall\_exit\_to\_user\_mode, perf\_event\_update\_userpage, entry\_SYSCALL\_64\_after\_hwframe, perf\_event\_groups\_first} |
| Exclusive | 1 | {\_\_dev\_queue\_xmit}, ,{schedule\_timeout} |
| 2 | {\_\_dev\_queue\_xmit, ip\_finish\_output2}, ,{ \_\_inet\_lookup\_established, schedule\_timeout} |
| 3 | {\_\_dev\_queue\_xmit, ip\_finish\_output2, kfree}, ,{kfree, \_\_inet\_lookup\_established, schedule\_timeout} |
| 4 | {\_\_dev\_queue\_xmit, ip\_finish\_output2, kfree, \_\_inet\_lookup\_established}, ,{ip\_finish\_output2, kfree, \_\_inet\_lookup\_established, schedule\_timeout} |
| 5 | {\_\_dev\_queue\_xmit, ip\_finish\_output2, kfree, \_\_inet\_lookup\_established, schedule\_timeout} |
| All | 1 | {psi\_group\_change}, ,{perf\_event\_groups\_first} |
| 2 | {psi\_group\_change, syscall\_exit\_to\_user\_mode}, ,{ entry\_SYSCALL\_64\_after\_hwframe, perf\_event\_groups\_first} |
| 3 | {psi\_group\_change, syscall\_exit\_to\_user\_mode, perf\_event\_update\_userpage}, ,{perf\_event\_update\_userpage, entry\_SYSCALL\_64\_after\_hwframe, perf\_event\_groups\_first} |
| 4 | {psi\_group\_change, syscall\_exit\_to\_user\_mode, perf\_event\_update\_userpage, entry\_SYSCALL\_64\_after\_hwframe}, ,{ syscall\_exit\_to\_user\_mode, perf\_event\_update\_userpage, entry\_SYSCALL\_64\_after\_hwframe, perf\_event\_groups\_first} |
| 5 | {psi\_group\_change, syscall\_exit\_to\_user\_mode, perf\_event\_update\_userpage, entry\_SYSCALL\_64\_after\_hwframe, perf\_event\_groups\_first} |
| Instruction | Common | 1 | {psi\_group\_change}, ,{perf\_event\_update\_userpage} |
| 2 | {psi\_group\_change, merge\_sched\_in}, ,{native\_sched\_clock, perf\_event\_update\_userpage} |
| 3 | {psi\_group\_change, merge\_sched\_in, event\_sched\_in}, ,{event\_sched\_in, native\_sched\_clock, perf\_event\_update\_userpage} |
| 4 | {psi\_group\_change, merge\_sched\_in, event\_sched\_in, native\_sched\_clock}, ,{merge\_sched\_in, event\_sched\_in, native\_sched\_clock, perf\_event\_update\_userpage} |
| 5 | {psi\_group\_change, merge\_sched\_in, event\_sched\_in, native\_sched\_clock, perf\_event\_update\_userpage} |
| Exclusive | 1 | {\_\_cgroup\_bpf\_run\_filter\_skb}, ,{timerqueue\_add} |
| 2 | {\_\_cgroup\_bpf\_run\_filter\_skb, \_\_dev\_queue\_xmit}, ,{\_\_ip\_queue\_xmit, timerqueue\_add} |
| 3 | {\_\_cgroup\_bpf\_run\_filter\_skb, \_\_dev\_queue\_xmit, do\_poll.constprop.0}, ,{do\_poll.constprop.0, \_\_ip\_queue\_xmit, timerqueue\_add} |
| 4 | {\_\_cgroup\_bpf\_run\_filter\_skb, \_\_dev\_queue\_xmit, do\_poll.constprop.0, \_\_ip\_queue\_xmit}, ,{\_\_dev\_queue\_xmit, do\_poll.constprop.0, \_\_ip\_queue\_xmit, timerqueue\_add} |
| 5 | {\_\_cgroup\_bpf\_run\_filter\_skb, \_\_dev\_queue\_xmit, do\_poll.constprop.0, \_\_ip\_queue\_xmit, timerqueue\_add} |
| All | 1 | {psi\_group\_change}, ,{perf\_event\_update\_userpage} |
| 2 | {psi\_group\_change, merge\_sched\_in}, ,{native\_sched\_clock, perf\_event\_update\_userpage} |
| 3 | {psi\_group\_change, merge\_sched\_in, event\_sched\_in}, ,{ event\_sched\_in, native\_sched\_clock, perf\_event\_update\_userpage} |
| 4 | {psi\_group\_change, merge\_sched\_in, event\_sched\_in, native\_sched\_clock}, ,{merge\_sched\_in, event\_sched\_in, native\_sched\_clock, perf\_event\_update\_userpage} |
| 5 | {psi\_group\_change, merge\_sched\_in, event\_sched\_in, native\_sched\_clock, perf\_event\_update\_userpage} |

Tables 23 and 24 show various combinations of Perf TOP features extracted from CS and GS. In Tables 21 and 22, we sort the symbols in Types 1 and 2 based on high ASR and low ASRD and list the symbols into the Top Five Symbols (TFS). In TFS, we sort the symbols by high ASR, extract the top 5 features, and sort them in reverse order by low ASRD. By choosing features with a high ASR, TFS is designed to get as many features as possible and minimize the loss of information by selecting a low ASRD.

The above formula is used to calculate TFS. In this study, n is 5, and the number of feature combinations created is 31. Since TFS is the sum of all combinations, the number of combinations for all features increases exponentially. Therefore, it is necessary to calculate an appropriate TFS value considering the importance according to ASR and ASRD. 16 Tables for each 23 and 24 are created according to the 16 attack scenarios in Table 2, respectively.

Figure 20. 50 symbols extracted by referring to the Perf Records of the CS

Figure 21. 50 symbols extracted by referring to the Perf Records of the CS

Figures 20 and 21 show averages of overheads of common symbols extracted from each of the three CS. The overhead information of these symbols is extracted from the Perf Records of each CS. The symbols are the same symbols found simultaneously in all the CS. The top 50 symbols were extracted in order of high overhead and sorted in descending order. Therefore, the graph patterns of these figures are monotonically decreasing. Figure 20 shows CS kernel overhead information collected under the attacks, and Figure 21 shows CS kernel overhead information collected in the normal EV authentication mode.

Figure 22. 50 symbols extracted by referring to the Perf Record of the GS

Figure 23. 50 symbols extracted by referring to the Perf Record of the GS

Figures 22 and 23 show overhead information of symbols extracted from the GS. Since there is only one GS in this study, the average of the overhead values ​​of the same symbol is not calculated like in Figures 20 and 21. The rest of Figures 22 and 23 are identical to Figures 20 and 21. Figures 20 to 23 show that the patterns of the graphs are all monotonically decreasing, and high overhead occurs in specific symbols in the front part.

Table 25. Comparison of the optimal numbers of clusters and silhouette scores using K Means clustering on the Averaged Perf Record of CS

(EP: Elbow Point, BSS: Best Silhouette Score, N/A: Not Available)

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Types  Scenario | Attack Mode | | | | | | Normal Mode | | | | | | EP Mean | BSS Mean | All EP Mean | All BSS Mean |
| Cycle | | Branch | | Instruction | | Cycle | | Branch | | Instruction | |
| EP | BSS | EP | BSS | EP | BSS | EP | BSS | EP | BSS | EP | BSS |
| cid\_rcoff\_goff | 6 | 0.991 | 4 | 0.99 | 3 | 0.994 | 9 | 0.926 | N/A | N/A | 2 | 0.884 | 4.8 | 0.957 | 4.361 | 0.947 |
| cid\_rcoff\_gon | 4 | 0.922 | N/A | N/A | 3 | 1 | 6 | 0.957 | N/A | N/A | N/A | N/A | 4.333 | 0.959 |
| cid\_rcon\_goff | 5 | 1 | 3 | 0.995 | 3 | 0.995 | 7 | 0.863 | 2 | 0.917 | 5 | 0.844 | 4.166 | 0.935 |
| cid\_rcon\_gon | 6 | 1 | 2 | 0.871 | 2 | 0.887 | 7 | 0.947 | 2 | 0.931 | 2 | 0.94 | 3.5 | 0.929 |
| wct\_rcoff\_goff | 6 | 0.992 | 3 | 0.994 | 3 | 0.995 | 7 | 0.958 | 2 | 0.847 | 4 | 0.893 | 4.166 | 0.946 |
| wct\_rcoff\_gon | 3 | 0.85 | N/A | N/A | 4 | 0.977 | 3 | 0.982 | 3 | 0.982 | 2 | 0.976 | 3 | 0.953 |
| wct\_rcon\_goff | 8 | 0.993 | 5 | 0.995 | 3 | 0.989 | 10 | 0.95 | N/A | N/A | 2 | 0.9 | 5.6 | 0.965 |
| wct\_rcon\_gon | 5 | 0.983 | 5 | 0.96 | 2 | 0.89 | 4 | 1 | 2 | 0.916 | 4 | 0.972 | 3.666 | 0.953 |
| wet\_rcoff\_goff | 6 | 1 | 4 | 0.995 | 4 | 0.99 | 3 | 1 | N/A | N/A | N/A | N/A | 4.25 | 0.996 |
| wet\_rcoff\_gon | 5 | 0.975 | 2 | 0.858 | N/A | N/A | 7 | 0.965 | N/A | N/A | 2 | 0.875 | 4 | 0.918 |
| wet\_rcon\_goff | 6 | 0.997 | 4 | 0.996 | 4 | 0.996 | 10 | 0.955 | 2 | 0.921 | 10 | 0.976 | 6 | 0.973 |
| wet\_rcon\_gon | 5 | 1 | N/A | N/A | 4 | 0.972 | 8 | 0.889 | 6 | 0.956 | 5 | 0.983 | 5.6 | 0.96 |
| wid\_rcoff\_goff | 8 | 0.992 | 4 | 0.988 | 3 | 0.971 | 7 | 0.873 | 2 | 0.886 | 2 | 0.873 | 4.333 | 0.93 |
| wid\_rcoff\_gon | 6 | 0.985 | N/A | N/A | 4 | 0.978 | 2 | 0.883 | 2 | 0.822 | 2 | 0.811 | 3.2 | 0.895 |
| wid\_rcon\_goff | 7 | 0.996 | 4 | 0.988 | 3 | 0.995 | 10 | 0.956 | 2 | 0.947 | 6 | 0.989 | 5.333 | 0.978 |
| wid\_rcon\_gon | 6 | 0.982 | 2 | 0.809 | 2 | 0.865 | 9 | 0.982 | 2 | 0.924 | 2 | 0.891 | 3.833 | 0.908 |

Table 26. Comparison of the optimal numbers of clusters and silhouette scores using K Means clustering on the Averaged Perf Record of GS

(EP: Elbow Point, BSS: Best Silhouette Score, N/A: Not Available)

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Types  Scenario | Attack Mode | | | | | | Normal Mode | | | | | | EP Mean | BSS Mean | All EP Mean | All BSS Mean |
| Cycle | | Branch | | Instruction | | Cycle | | Branch | | Instruction | |
| EP | BSS | EP | BSS | EP | BSS | EP | BSS | EP | BSS | EP | BSS |
| cid\_rcoff\_goff | 33 | 0.935 | 2 | 0.958 | 2 | 0.975 | 2 | 0.872 | 2 | 0.923 | 2 | 0.964 | 7.166 | 0.937 | 5.135 | 0.907 |
| cid\_rcoff\_gon | 2 | 0.872 | 2 | 0.923 | 2 | 0.964 | 19 | 0.938 | 2 | 0.92 | 2 | 0.948 | 4.833 | 0.927 |
| cid\_rcon\_goff | 2 | 0.884 | 2 | 0.965 | 2 | 0.976 | 2 | 0.883 | 2 | 0.922 | 2 | 0.96 | 2 | 0.931 |
| cid\_rcon\_gon | 19 | 0.783 | 2 | 0.912 | 2 | 0.928 | 18 | 0.839 | 2 | 0.923 | 2 | 0.915 | 7.5 | 0.883 |
| wct\_rcoff\_goff | 31 | 0.87 | 2 | 0.963 | 2 | 0.971 | 2 | 0.885 | 2 | 0.923 | 2 | 0.934 | 6.833 | 0.924 |
| wct\_rcoff\_gon | 2 | 0.81 | 10 | 0.779 | 12 | 0.835 | 25 | 0.948 | 13 | 0.952 | 2 | 0.908 | 10.666 | 0.872 |
| wct\_rcon\_goff | 2 | 0.894 | 2 | 0.966 | 2 | 0.974 | 2 | 0.886 | 2 | 0.945 | 2 | 0.967 | 2 | 0.938 |
| wct\_rcon\_gon | 2 | 0.821 | 13 | 0.86 | 2 | 0.944 | 20 | 0.908 | 2 | 0.953 | 2 | 0.935 | 6.833 | 0.903 |
| wet\_rcoff\_goff | 2 | 0.864 | 2 | 0.884 | 2 | 0.962 | 2 | 0.871 | 2 | 0.92 | 2 | 0.949 | 2 | 0.908 |
| wet\_rcoff\_gon | 2 | 0.75 | 13 | 0.907 | 2 | 0.938 | 25 | 0.94 | 9 | 0.805 | 2 | 0.942 | 8.833 | 0.88 |
| wet\_rcon\_goff | 2 | 0.844 | 2 | 0.94 | 2 | 0.957 | 2 | 0.86 | 2 | 0.952 | 2 | 0.957 | 2 | 0.918 |
| wet\_rcon\_gon | 2 | 0.76 | 2 | 0.907 | N/A | N/A | 2 | 0.76 | 2 | 0.907 | N/A | N/A | 2 | 0.833 |
| wid\_rcoff\_goff | 2 | 0.89 | 2 | 0.963 | 2 | 0.974 | 2 | 0.875 | 2 | 0.92 | 2 | 0.942 | 2 | 0.927 |
| wid\_rcoff\_gon | 2 | 0.83 | 2 | 0.909 | 2 | 0.941 | 2 | 0.885 | 13 | 0.992 | 2 | 0.916 | 3.833 | 0.912 |
| wid\_rcon\_goff | 25 | 0.867 | 2 | 0.963 | 2 | 0.973 | 21 | 0.878 | 2 | 0.922 | 2 | 0.961 | 9 | 0.937 |
| wid\_rcon\_gon | 2 | 0.779 | 2 | 0.811 | 2 | 0.94 | 18 | 0.849 | 2 | 0.893 | 2 | 0.958 | 4.666 | 0.927 |

Figures 25 and 26 show the result of finding an elbow point location on the CS and GS Perf Record. As shown in Figures 20 to 23, the Perf Record overheads are sorted in descending order based on the overhead size of symbols, so there is a section where the overheads decrease rapidly and converge to 0. Silhouette scores [42] are calculated after running K Means clustering [43] several times while gradually increasing the K value. The K value is the "symbol index" value in Figures 20 and 23. The score is used to gauge clustering quality on the overheads of the Perf Records. The Silhouette score method generates a high score when the level of the K fits the clustering results. In other words, the silhouette score is the highest in the section where the overhead change rate is large because the decision boundary can be clearly divided during clustering. In this sense, a K value with the highest score considers a "symbol index" position as an elbow point. In this experiment, we used the K means library provided by Python's Scikit-Learn [44], and all parameter values ​​were applied as default values. In CS and GS, the average EP for each scenario and the total average EP are calculated for all scenarios. Since the TFS values of the CS and GS are 4.361 and 5.135, the number of important symbols with significant overhead can be considered five by TFS.

Table 27. The total number of CS Perf Record symbols and ideal sampled symbol count

(RSC: Record Symbol Count, CC: Cluster Count)

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Types  Scenario | Attack | | | | | | Normal | | | | | |
| Cycle | | Branch | | Instructions | | Cycle | | Branch | | Instructions | |
| RSC | CC | RSC | CC | RSC | CC | RSC | CC | RSC | CC | RSC | CC |
| cid\_rcoff\_goff | 288 | 18 | 207 | 14 | 186 | 9 | 75 | 8 | 56 | 0 | 70 | 2 |
| cid\_rcoff\_gon | 66 | 3 | 36 | 0 | 38 | 2 | 69 | 9 | 58 | 0 | 49 | 0 |
| cid\_rcon\_goff | 364 | 100 | 228 | 29 | 222 | 23 | 91 | 6 | 79 | 4 | 78 | 4 |
| cid\_rcon\_gon | 89 | 7 | 64 | 1 | 63 | 1 | 86 | 6 | 77 | 2 | 75 | 1 |
| wct\_rcoff\_goff | 271 | 19 | 189 | 16 | 208 | 12 | 77 | 6 | 40 | 2 | 51 | 3 |
| wct\_rcoff\_gon | 79 | 2 | 46 | 0 | 44 | 3 | 85 | 2 | 58 | 3 | 63 | 1 |
| wct\_rcon\_goff | 309 | 29 | 231 | 54 | 234 | 43 | 85 | 10 | 68 | 0 | 64 | 2 |
| wct\_rcon\_gon | 62 | 8 | 50 | 4 | 48 | 1 | 106 | 9 | 76 | 1 | 72 | 10 |
| wet\_rcoff\_goff | 253 | 27 | 201 | 3 | 201 | 22 | 142 | 8 | 98 | 0 | 104 | 0 |
| wet\_rcoff\_gon | 62 | 4 | 48 | 1 | 40 | 0 | 58 | 6 | 54 | 0 | 46 | 1 |
| wet\_rcon\_goff | 372 | 28 | 265 | 52 | 276 | 37 | 150 | 9 | 119 | 2 | 129 | 9 |
| wet\_rcon\_gon | 59 | 4 | 39 | 0 | 37 | 3 | 54 | 7 | 58 | 5 | 59 | 5 |
| wid\_rcoff\_goff | 284 | 39 | 209 | 3 | 183 | 2 | 64 | 7 | 47 | 1 | 56 | 3 |
| wid\_rcoff\_gon | 69 | 9 | 55 | 0 | 46 | 3 | 72 | prff | 56 | 3 | 53 | 3 |
| wid\_rcon\_goff | 319 | 25 | 213 | 3 | 214 | 49 | 116 | 16 | 90 | 1 | 95 | 8 |
| wid\_rcon\_gon | 58 | 6 | 42 | 2 | 42 | 1 | 58 | 8 | 62 | 1 | 51 | 2 |

Table 28. The total number of GS Perf Record symbols and ideal sampled symbol count

(RSC: Record Symbol Count, SSC: Sampled Symbol Count)

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Types  Scenario | Attack | | | | | | Normal | | | | | |
| Cycle | | Branch | | Instructions | | Cycle | | Branch | | Instructions | |
| RSC | CC | RSC | CC | RSC | CC | RSC | CC | RSC | CC | RSC | CC |
| cid\_rcoff\_goff | 449 | 32 | 429 | 30 | 424 | 16 | 270 | 16 | 207 | 13 | 221 | 6 |
| cid\_rcoff\_gon | 270 | 16 | 207 | 13 | 221 | 6 | 221 | 18 | 160 | 12 | 166 | 4 |
| cid\_rcon\_goff | 407 | 29 | 400 | 19 | 385 | 12 | 241 | 13 | 208 | 7 | 202 | 5 |
| cid\_rcon\_gon | 152 | 18 | 129 | 7 | 146 | 6 | 202 | 17 | 173 | 10 | 155 | 6 |
| wct\_rcoff\_goff | 454 | 30 | 437 | 26 | 441 | 17 | 258 | 18 | 211 | 12 | 208 | 9 |
| wct\_rcoff\_gon | 184 | 13 | 159 | 10 | 159 | 12 | 224 | 24 | 163 | 12 | 1558 | 9 |
| wct\_rcon\_goff | 400 | 25 | 396 | 12 | 379 | 13 | 286 | 16 | 222 | 12 | 217 | 5 |
| wct\_rcon\_gon | 168 | 14 | 141 | 12 | 132 | 6 | 237 | 19 | 185 | 9 | 196 | 5 |
| wet\_rcoff\_goff | 235 | 17 | 195 | 11 | 201 | 6 | 270 | 19 | 229 | 12 | 226 | 7 |
| wet\_rcoff\_gon | 151 | 13 | 136 | 12 | 136 | 6 | 211 | 24 | 144 | 8 | 149 | 3 |
| wet\_rcon\_goff | 222 | 19 | 179 | 10 | 183 | 7 | 261 | 18 | 211 | 9 | 200 | 8 |
| wet\_rcon\_gon | 168 | 13 | 88 | 8 | 127 | 0 | 168 | 13 | 88 | 8 | 127 | 0 |
| wid\_rcoff\_goff | 456 | 30 | 426 | 24 | 431 | 13 | 272 | 21 | 220 | 12 | 12 | 4 |
| wid\_rcoff\_gon | 183 | 13 | 134 | 9 | 131 | 4 | 239 | 13 | 179 | 12 | 190 | 7 |
| wid\_rcon\_goff | 408 | 24 | 389 | 20 | 389 | 12 | 271 | 20 | 216 | 11 | 215 | 7 |
| wid\_rcon\_gon | 171 | 13 | 168 | 9 | 143 | 4 | 202 | 17 | 155 | 8 | 167 | 3 |

Tables 27 and 28 show the total number of symbols (RSC) in Perf Record and the number of clusters (CC) used in K-means clustering. We calculate the RSC's arithmetic mean and standard deviation and add them together to get a Boundary based on the Arithmetic Average and Standard Deviation (BAS). The formula for calculating BAS is:

* when

With this added value as a boundary, symbols with overhead greater than this value are extracted from the RSC population. The number of the symbols to be extracted is set in the range of the cluster count K. The K means clustering and silhouette score are implemented starting from K = 2 several times, increasing one to the count until its K reaches BAS.

### Proof

Let Symbol Overhead List (SOL), . Since is sorted in descending order; the list satisfies the monotonically decreasing set. cf., According to the monotone convergence theorem [45], we can define:

1. def., If is a monotonically increasing sequence and bounded upward, then converges and meets
2. def., If is a monotonically decreasing sequence and is bounded downward, then converges and meets
3. s.t., By categories 1 and 2, bounded monotonic sequences are proven to converge.

pf., From Category 1, let . Since the sequence is bounded upward, has an upper bound, cf., according to the completeness of the real numbers [46]. Let . Then, we need to prove . For any positive number , is not an upper bound of , there exists a natural number . Since is a monotonically increasing sequence, and is the upper bound of , the following equation holds when : . i.e., . Consequently, and . Since , . From Category 2, let , and be a monotonically increasing sequence. By Category 1, then, . . Since , . Q.E.D., it is proved that is a monotonically decreasing sequence.

According to the definition of K Means clustering [47], there is the proper number of clusters, for . The paper suggests finding an elbow point on data points by calculating the Silhouette Score (SS) [48]. cf.., ,, . When the score is the maximum, indicates the optimal elbow point. S.t., . The silhouette score is higher when the average distance of data within the same cluster is small and the distance between different clusters is large. As demonstrated above, the magnitudes of the symbol overheads are distributed in a monotonically decreasing pattern. In Tables 27 and 28, symbols having an overhead size larger than the boundary of BAS in RSC are shown in CC. In Tables 25 and 26, "All BSS Mean" values are 0947 and 0.907, respectively, showing a high average score of 90% or more. The overheads are monotonically decreasing and are extracted from the range that satisfies the BAS boundary. cond., when , s.t., 0.996, 0.8720.938.

Table 29. Final combined feature information for CS under the CID\_RCOFF\_GOFF attack scenario (TFCC: Total Feature Combination Count, CSR: Combined Sampling Resolution)

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Type 1 | Type 2 | TFCC | Set Size | Symbol Set | Type 3 | CSR |
| Branch | Common | 31 | 1 | ['psi\_group\_change'] | Attack | 0.432 |
| Normal | 0.189 |
|  | | |
| ['kmem\_cache\_alloc\_trace'] | Attack | 0.181 |
| Normal | 0.076 |
|  | | | |
| 5 | ['psi\_group\_change', 'perf\_event\_groups\_insert', 'event\_sched\_in', 'merge\_sched\_in', 'kmem\_cache\_alloc\_trace'] | Attack | 0.358 |
| Normal | 0.191 |
| Exclusive | 31 | 1 | ['kfree'] | Attack | 0.281 |
| Normal | 0 |
|  | | |
| ['kmem\_cache\_alloc\_node\_trace'] | Attack | 0.169 |
| Normal | 0 |
|  | | | |
| 5 | ['kfree', 'inherit\_event.constprop.0', 'rb\_next', 'perf\_event\_alloc', 'kmem\_cache\_alloc\_node\_trace'] | Attack | 0.322 |
| Normal | 0 |
| All | 31 | 1 | ['kfree'] | Attack | 0.281 |
| Normal | 0 |
|  | | |
| ['rb\_next'] | Attack | 0.205 |
| Normal | 0 |
|  | | | |
| 5 | ['kfree', 'psi\_group\_change', 'inherit\_event.constprop.0', 'perf\_event\_groups\_insert', 'rb\_next'] | Attack | 0.398 |
| Normal | 0.086 |
| Cycle | Common | 1 | 1 | ['perf\_event\_alloc'] | Attack | 0.385 |
| Normal | 0.076 |
| Exclusive | 31 | 1 | ['memset\_erms'] | Attack | 0.359 |
| Normal | 0 |
|  | | |
| ['psi\_group\_change'] | Attack | 0.163 |
| Normal | 0 |
|  | | | |
| 5 | ['memset\_erms', 'rb\_next', 'inherit\_event.constprop.0', 'kfree', 'psi\_group\_change'] | Attack | 0.33 |
| Normal | 0 |
| All | 31 | 1 | ['memset\_erms'] | Attack | 0.359 |
| Normal | 0 |
|  | | |
| ['kfree'] | Attack | 0.207 |
| Normal | 0 |
|  | | | |
| 5 | ['memset\_erms', 'rb\_next', 'perf\_event\_alloc', 'inherit\_event.constprop.0', 'kfree'] | Attack | 0.386 |
| Normal | 0.025 |
| Instruction | Common | 31 | 1 | ['psi\_group\_change'] | Attack | 0.346 |
| Normal | 0.143 |
|  | | |
| ['x86\_pmu\_event\_init'] | Attack | 0.11 |
| Normal | 0.077 |
|  | | | |
| 5 | ['psi\_group\_change', 'event\_sched\_in', 'inherit\_event.constprop.0', 'native\_sched\_clock', 'x86\_pmu\_event\_init'] | Attack | 0.292 |
| Normal | 0.174 |
| Exclusive | 31 | 1 | ['kfree'] | Attack | 0.356 |
| Normal | 0 |
|  | | |
| ['kmem\_cache\_alloc\_node\_trace'] | Attack | 0.207 |
| Normal | 0 |
|  | | | |
| 5 | ['kfree', 'perf\_event\_alloc', 'merge\_sched\_in', 'kmem\_cache\_alloc\_node', 'kmem\_cache\_alloc\_node\_trace'] | Attack | 0.383 |
| Normal | 0 |
| All | 31 | 1 | ['kfree'] | Attack | 0.356 |
| Normal | 0 |
|  | | |
| ['kmem\_cache\_alloc\_node'] | Attack | 0.208 |
| Normal | 0 |
|  | | | |
| 5 | ['kfree', 'perf\_event\_alloc', 'psi\_group\_change', 'merge\_sched\_in', 'kmem\_cache\_alloc\_node'] | Attack | 0.402 |
| Normal | 0.047 |

Table 30. Final combined feature information for GS under the CID\_RCOFF\_GOFF attack scenario (TFCC: Total Feature Combination Count, CSR: Combined Sampling Resolution)

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Type 1 | Type 2 | TFCC | Set Size | Symbol Set | Type 3 | CSR |
| Branch | Common | 31 | 1 | ['psi\_group\_change'] | Attack | 0.469 |
| Normal | 0.447 |
|  | | |
| ['rb\_next'] | Attack | 0.251 |
| Normal | 0.291 |
|  | | | |
| 5 | ['psi\_group\_change', 'merge\_sched\_in', 'event\_sched\_in', 'visit\_groups\_merge.constprop.0.is', 'rb\_next'] | Attack | 0.479 |
| Normal | 0.525 |
| Exclusive | 31 | 1 | ['\_\_cgroup\_bpf\_run\_filter\_skb'] | Attack | 0.129 |
| Normal | 0 |
|  | | |
| ['skb\_release\_data'] | Attack | 0.087 |
| Normal | 0 |
|  | | | |
| 5 | ['\_\_cgroup\_bpf\_run\_filter\_skb', 'timerqueue\_add', 'kmem\_cache\_free', 'tcp\_write\_xmit', 'skb\_release\_data'] | Attack | 0.132 |
| Normal | 0.028 |
| All | 31 | 1 | ['psi\_group\_change'] | Attack | 0.469 |
| Normal | 0.447 |
|  | | |
| ['rb\_next'] | Attack | 0.251 |
| Normal | 0.291 |
|  | | | |
| 5 | ['psi\_group\_change', 'merge\_sched\_in', 'event\_sched\_in', 'visit\_groups\_merge.constprop.0.is', 'rb\_next'] | Attack | 0.479 |
| Normal | 0.525 |
| Cycle | Common | 31 | 1 | ['psi\_group\_change'] | Attack | 0.434 |
| Normal | 0.343 |
|  | | |
| ['perf\_event\_groups\_first'] | Attack | 0.388 |
| Normal | 0.27 |
|  | | | |
| 5 | ['psi\_group\_change', 'syscall\_exit\_to\_user\_mode', 'perf\_event\_update\_userpage', 'entry\_SYSCALL\_64\_after\_hwframe', 'perf\_event\_groups\_first'] | Attack | 0.526 |
| Normal | 0.486 |
| Exclusive | 31 | 1 | ['\_\_dev\_queue\_xmit'] | Attack | 0.124 |
| Normal | 0 |
|  | | |
| ['schedule\_timeout'] | Attack | 0.037 |
| Normal | 0 |
|  | | | |
| 5 | ['\_\_dev\_queue\_xmit', 'ip\_finish\_output2', 'kfree', '\_\_inet\_lookup\_established', 'schedule\_timeout'] | Normal | 0.103 |
| Attack | 0 |
| All | 31 | 1 | ['psi\_group\_change'] | Attack | 0.434 |
| Normal | 0.343 |
|  | | |
| ['perf\_event\_groups\_first'] | Attack | 0.388 |
| Normal | 0.27 |
|  | | | |
| 5 | ['psi\_group\_change', 'syscall\_exit\_to\_user\_mode', 'perf\_event\_update\_userpage', 'entry\_SYSCALL\_64\_after\_hwframe', 'perf\_event\_groups\_first'] | Attack | 0.526 |
| Normal | 0.486 |
| Instruction | Common | 31 | 1 | ['psi\_group\_change'] | Attack | 0.476 |
| Normal | 0.435 |
|  | | |
| ['perf\_event\_update\_userpage'] | Attack | 0.206 |
| Normal | 0.307 |
|  | | | |
| 5 | ['psi\_group\_change', 'merge\_sched\_in', 'event\_sched\_in', 'native\_sched\_clock', 'perf\_event\_update\_userpage'] | Attack | 0.418 |
| Normal | 0.52 |
| Exclusive | 31 | 1 | ['\_\_cgroup\_bpf\_run\_filter\_skb'] | Attack | 0.218 |
| Normal | 0 |
|  | | |
| ['timerqueue\_add'] | Attack | 0 |
| Normal | 0.096 |
|  | | | |
| 5 | ['\_\_cgroup\_bpf\_run\_filter\_skb', '\_\_dev\_queue\_xmit', 'do\_poll.constprop.0', '\_\_ip\_queue\_xmit', 'timerqueue\_add'] | Attack | 0.121 |
| Normal | 0.086 |
| All | 31 | 1 | ['psi\_group\_change'] | Attack | 0.476 |
| Normal | 0.435 |
|  | | |
| ['perf\_event\_update\_userpage'] | Attack | 0.206 |
| Normal | 0.307 |
|  | | | |
| 5 | ['psi\_group\_change', 'merge\_sched\_in', 'event\_sched\_in', 'native\_sched\_clock', 'perf\_event\_update\_userpage'] | Attack | 0.418 |
| Normal | 0.52 |

Tables 29 and 30 show feature combinations and CSRs extracted for CS and GS by feature engineering. “TFCC” is 31 when "n" is 5 in TFS. "Set Size" means the number of symbols in an individual feature combination. "CSR" calculates information loss caused by feature downsizing when different symbols are combined into one feature combination. "CSR" is calculated as follows.

* CSR =

"n" means the number of symbols belonging to each feature combination. A higher "CSR" means a better feature combination because the information loss is lower. Conversely, the lower the "CSR," the greater the loss of information. Therefore, a reasonable classification model can be created by selecting features with a low “CSR” value rather than unconditionally selecting features with a high F1 score from various ML classifiers. These tables are created 16 each for a total of 16 scenarios.

Table 31. Final basic feature sizes of CS under all the attack scenarios (N/A: Not Available)

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Scenario | Type 1 | Type 2 | Type 3 | Value | | | | |
| cid\_rcoff\_goff | Branch | Common | Feature Name | psi\_group\_change | perf\_event\_groups\_insert | event\_sched\_in | merge\_sched\_in | kmem\_cache\_alloc\_trace |
| Attack | 330 | 193 | 104 | 159 | 123 |
| Normal | 115 | 64 | 125 | 55 | 24 |
| Exclusive | Feature Name | kfree | inherit\_event.constprop.0 | rb\_next | perf\_event\_alloc | kmem\_cache\_alloc\_node\_trace |
| Attack | 189 | 132 | 151 | 96 | 102 |
| Normal | 189 | 132 | 151 | 96 | 102 |
| All | Feature Name | kfree | psi\_group\_change | inherit\_event.constprop.0 | perf\_event\_groups\_insert | rb\_next |
| Attack | 189 | 330 | 132 | 193 | 151 |
| Normal | 189 | 115 | 132 | 6 | 151 |
| Cycles | Common | Feature Name | perf\_event\_alloc | N/A | N/A | N/A | N/A |
| Attack | 291 | N/A | N/A | N/A | N/A |
| Normal | 12 | N/A | N/A | N/A | N/A |
| Exclusive | Feature Name | memset\_erms | rb\_next | inherit\_event.constprop.0 | kfree | psi\_group\_change |
| Attack | 264 | 163 | 115 | 138 | 65 |
| Normal | 264 | 163 | 115 | 138 | 65 |
| All | Feature Name | memset\_erms | perf\_event\_alloc | inherit\_event.constprop.0 | kfree | N/A |
| Attack | 163 | 291 | 115 | 138 | N/A |
| Normal | 163 | 12 | 115 | 138 | N/A |
| Instructions | Common | Feature Name | psi\_group\_change | event\_sched\_in | inherit\_event.constprop.0 | native\_sched\_clock | x86\_pmu\_event\_init |
| Attack | 255 | 138 | 136 | 54 | 73 |
| Normal | 84 | 12 | 83 | 25 | 44 |
| Exclusive | Feature Name | kfree | perf\_event\_alloc | merge\_sched\_in | kmem\_cache\_alloc\_node | kmem\_cache\_alloc\_node\_trace |
| Attack | 271 | 236 | 137 | 129 | 147 |
| Normal | 271 | 236 | 137 | 129 | 147 |
| All | Feature Name | kfree | perf\_event\_alloc | psi\_group\_change | merge\_sched\_in | kmem\_cache\_alloc\_node |
| Attack | 271 | 236 | 255 | 137 | 129 |
| Normal | 271 | 236 | 84 | 137 | 129 |
| cid\_rcoff\_gon | Branch | Common | Feature Name | N/A | N/A | N/A | N/A | N/A |
| Attack | N/A | N/A | N/A | N/A | N/A |
| Normal | N/A | N/A | N/A | N/A | N/A |
| Exclusive | Feature Name | psi\_group\_change | event\_sched\_in | inherit\_event.constprop.0 | merge\_sched\_in | visit\_groups\_merge.constprop.0.is |
| Attack | 22 | 22 | 17 | 17 | 3 |
| Normal | 22 | 22 | 17 | 17 | 3 |
| All | Feature Name | psi\_group\_change | event\_sched\_in | inherit\_event.constprop.0 | merge\_sched\_in | visit\_groups\_merge.constprop.0.is |
| Attack | 22 | 22 | 17 | 17 | 3 |
| Normal | 22 | 22 | 17 | 17 | 3 |
| Cycles | Common | Feature Name | native\_write\_msr | N/A | N/A | N/A | N/A |
| Attack | 1 | N/A | N/A | N/A | N/A |
| Normal | 1 | N/A | N/A | N/A | N/A |
| Exclusive | Feature Name | syscall\_return\_via\_sysret | syscall\_exit\_to\_user\_mode | N/A | N/A | N/A |
| Attack | 18 | 2 | N/A | N/A | N/A |
| Normal | 18 | 2 | N/A | N/A | N/A |
| All | Feature Name | syscall\_return\_via\_sysret | syscall\_exit\_to\_user\_mode | native\_write\_msr | N/A | N/A |
| Attack | 18 | 2 | 1 | N/A | N/A |
| Normal | 18 | 2 | 1 | N/A | N/A |
| Instructions | Common | Feature Name | N/A | N/A | N/A | N/A | N/A |
| Attack | N/A | N/A | N/A | N/A | N/A |
| Normal | N/A | N/A | N/A | N/A | N/A |
| Exclusive | Feature Name | kfree | perf\_event\_update\_userpage | event\_sched\_in | iterate\_groups | \_\_srcu\_read\_lock |
| Attack | 15 | 12 | 11 | 3 | 3 |
| Normal | 15 | 12 | 11 | 3 | 3 |
| All | Feature Name | kfree | perf\_event\_update\_userpage | event\_sched\_in | iterate\_groups | \_\_srcu\_read\_lock |
| Attack | 15 | 12 | 11 | 3 | 3 |
| Normal | 15 | 12 | 11 | 3 | 3 |
| cid\_rcon\_goff | Branch | Common | Feature Name | psi\_group\_change | event\_sched\_in | merge\_sched\_in | kmem\_cache\_alloc\_node\_trace | kmem\_cache\_alloc\_trace |
| Attack | 138 | 27 | 76 | 59 | 39 |
| Normal | 77 | 71 | 69 | 29 | 9 |
| Exclusive | Feature Name | perf\_event\_groups\_insert | kfree | kmem\_cache\_alloc\_node | perf\_event\_alloc | memset\_erms |
| Attack | 123 | 98 | 76 | 74 | 58 |
| Normal | 123 | 98 | 76 | 74 | 58 |
| All | Feature Name | perf\_event\_groups\_insert | psi\_group\_change | kfree | kmem\_cache\_alloc\_node | perf\_event\_alloc |
| Attack | 123 | 138 | 98 | 76 | 74 |
| Normal | 123 | 77 | 98 | 76 | 74 |
| Cycles | Common | Feature Name | memset\_erms | psi\_group\_change | syscall\_exit\_to\_user\_mode | perf\_event\_update\_userpage | entry\_SYSCALL\_64\_after\_hwframe |
| Attack | 138 | 77 | 57 | 60 | 50 |
| Normal | 122 | 122 | 113 | 123 | 120 |
| Exclusive | Feature Name | perf\_event\_alloc | perf\_iterate\_ctx | x86\_pmu\_event\_init | \_\_\_slab\_alloc | kmem\_cache\_alloc\_node\_trace |
| Attack | 104 | 16 | 53 | 26 | 22 |
| Normal | 104 | 16 | 53 | 26 | 22 |
| All | Feature Name | perf\_event\_alloc | memset\_erms | psi\_group\_change | syscall\_exit\_to\_user\_mode | perf\_event\_update\_userpage |
| Attack | 104 | 138 | 77 | 57 | 60 |
| Normal | 104 | 122 | 122 | 113 | 123 |
| Instructions | Common | Feature Name | psi\_group\_change | perf\_event\_alloc | kfree | kmem\_cache\_alloc\_node | merge\_sched\_in |
| Attack | 99 | 86 | 135 | 90 | 88 |
| Normal | 87 | 87 | 24 | 12 | 28 |
| Exclusive | Feature Name | memcg\_slab\_free\_hook | perf\_event\_groups\_insert | x86\_pmu\_event\_init | copy\_process | inherit\_event.constprop.0 |
| Attack | 111 | 73 | 67 | 80 | 72 |
| Normal | 111 | 73 | 67 | 80 | 72 |
| All | Feature Name | psi\_group\_change | memcg\_slab\_free\_hook | perf\_event\_alloc | kfree | perf\_event\_groups\_insert |
| Attack | 99 | 111 | 86 | 135 | 73 |
| Normal | 87 | 111 | 87 | 24 | 73 |
|  | Branch | Common | Feature Name | N/A | N/A | N/A | N/A | N/A |
| Attack | N/A | N/A | N/A | N/A | N/A |
| Normal | N/A | N/A | N/A | N/A | N/A |
| Exclusive | Feature Name | psi\_group\_change | merge\_sched\_in | inherit\_event.constprop.0 | native\_sched\_clock | memcg\_slab\_post\_alloc\_hook |
| Attack | 20 | 26 | 18 | 19 | 5 |
| Normal | 20 | 26 | 18 | 19 | 5 |
| All | Feature Name | psi\_group\_change | merge\_sched\_in | inherit\_event.constprop.0 | native\_sched\_clock | memcg\_slab\_post\_alloc\_hook |
| Attack | 20 | 26 | 18 | 19 | 5 |
| Normal | 20 | 26 | 18 | 19 | 5 |
| Cycles | Common | Feature Name | N/A | N/A | N/A | N/A | N/A |
| Attack | N/A | N/A | N/A | N/A | N/A |
| Normal | N/A | N/A | N/A | N/A | N/A |
| Exclusive | Feature Name | psi\_group\_change | syscall\_exit\_to\_user\_mode | memset\_erms | merge\_sched\_in | inherit\_task\_group.isra.0 |
| Attack | 27 | 26 | 27 | 18 | 14 |
| Normal | 27 | 26 | 27 | 18 | 14 |
| All | Feature Name | psi\_group\_change | syscall\_exit\_to\_user\_mode | memset\_erms | merge\_sched\_in | inherit\_task\_group.isra.0 |
| Attack | 27 | 26 | 27 | 18 | 14 |
| Normal | 27 | 26 | 27 | 18 | 14 |
| Instructions | Common | Feature Name | N/A | N/A | N/A | N/A | N/A |
| Attack | N/A | N/A | N/A | N/A | N/A |
| Normal | N/A | N/A | N/A | N/A | N/A |
| Exclusive | Feature Name | psi\_group\_change | perf\_event\_alloc | inherit\_event.constprop.0 | event\_sched\_in | kfree |
| Attack | 22 | 21 | 20 | 18 | 8 |
| Normal | 22 | 21 | 20 | 18 | 8 |
| All | Feature Name | psi\_group\_change | perf\_event\_alloc | inherit\_event.constprop.0 | event\_sched\_in | kfree |
| Attack | 22 | 21 | 20 | 18 | 8 |
| Normal | 22 | 21 | 20 | 18 | 8 |
| wct\_rcoff\_goff | Branch | Common | Feature Name | perf\_event\_alloc | event\_sched\_in | kmem\_cache\_alloc\_node\_trace | N/A | N/A |
| Attack | 127 | 95 | 68 | N/A | N/A |
| Normal | 11 | 2 | 47 | N/A | N/A |
| Exclusive | Feature Name | psi\_group\_change | kfree | perf\_event\_groups\_insert | memset\_erms | merge\_sched\_in |
| Attack | 316 | 232 | 198 | 118 | 74 |
| Normal | 316 | 232 | 198 | 118 | 74 |
| All | Feature Name | psi\_group\_change | kfree | perf\_event\_groups\_insert | memset\_erms | merge\_sched\_in |
| Attack | 316 | 232 | 198 | 118 | 74 |
| Normal | 316 | 232 | 198 | 118 | 74 |
| Cycles | Common | Feature Name | native\_write\_msr | N/A | N/A | N/A | N/A |
| Attack | 1 | N/A | N/A | N/A | N/A |
| Normal | 1 | N/A | N/A | N/A | N/A |
| Exclusive | Feature Name | memset\_erms | perf\_event\_alloc | inherit\_event.constprop.0 | syscall\_exit\_to\_user\_mode | perf\_event\_update\_userpage |
| Attack | 190 | 264 | 92 | 138 | 131 |
| Normal | 190 | 264 | 92 | 138 | 131 |
| All | Feature Name | memset\_erms | perf\_event\_alloc | inherit\_event.constprop.0 | syscall\_exit\_to\_user\_mode | perf\_event\_update\_userpage |
| Attack | 190 | 264 | 92 | 138 | 131 |
| Normal | 190 | 264 | 92 | 138 | 131 |
| Instructions | Common | Feature Name | N/A | N/A | N/A | N/A | N/A |
| Attack | N/A | N/A | N/A | N/A | N/A |
| Normal | N/A | N/A | N/A | N/A | N/A |
| Exclusive | Feature Name | psi\_group\_change | kfree | perf\_event\_alloc | memset\_erms | merge\_sched\_in |
| Attack | 274 | 209 | 164 | 135 | 126 |
| Normal | 274 | 209 | 164 | 135 | 126 |
| All | Feature Name | psi\_group\_change | kfree | perf\_event\_alloc | memset\_erms | merge\_sched\_in |
| Attack | 274 | 209 | 164 | 135 | 126 |
| Normal | 274 | 209 | 164 | 135 | 126 |
| wct\_rcoff\_gon | Branch | Common | Feature Name | psi\_group\_change | x86\_pmu\_enable | N/A | N/A | N/A |
| Attack | 6 | 1 | N/A | N/A | N/A |
| Normal | 26 | 1 | N/A | N/A | N/A |
| Exclusive | Feature Name | event\_sched\_in | kfree | merge\_sched\_in | perf\_iterate\_ctx | rb\_next |
| Attack | 20 | 8 | 4 | 2 | 1 |
| Normal | 20 | 8 | 4 | 2 | 1 |
| All | Feature Name | event\_sched\_in | psi\_group\_change | kfree | merge\_sched\_in | perf\_iterate\_ctx |
| Attack | 20 | 6 | 8 | 4 | 2 |
| Normal | 20 | 26 | 8 | 4 | 2 |
| Cycles | Common | Feature Name | perf\_event\_update\_userpage | memset\_erms | syscall\_exit\_to\_user\_mode | entry\_SYSCALL\_64\_after\_hwframe | perf\_event\_alloc |
| Attack | 4 | 3 | 4 | 3 | 4 |
| Normal | 34 | 27 | 1 | 1 | 3 |
| Exclusive | Feature Name | \_\_perf\_event\_task\_sched\_in | merge\_sched\_in | visit\_groups\_merge.constprop.0.is | kfree | native\_sched\_clock |
| Attack | 3 | 4 | 2 | 3 | 4 |
| Normal | 3 | 4 | 2 | 3 | 4 |
| All | Feature Name | perf\_event\_update\_userpage | memset\_erms | \_\_perf\_event\_task\_sched\_in | merge\_sched\_in | visit\_groups\_merge.constprop.0.is |
| Attack | 4 | 3 | 3 | 4 | 2 |
| Normal | 34 | 27 | 3 | 4 | 2 |
| Instructions | Common | Feature Name | perf\_event\_alloc | \_\_intel\_pmu\_enable\_all.constprop. | N/A | N/A | N/A |
| Attack | 7 | 1 | N/A | N/A | N/A |
| Normal | 3 | 1 | N/A | N/A | N/A |
| Exclusive | Feature Name | psi\_group\_change | kfree | perf\_event\_groups\_insert | rb\_next | memcg\_slab\_free\_hook |
| Attack | 12 | 17 | 4 | 4 | 4 |
| Normal | 12 | 17 | 4 | 4 | 4 |
| All | Feature Name | psi\_group\_change | kfree | perf\_event\_alloc | perf\_event\_groups\_insert | rb\_next |
| Attack | 12 | 17 | 7 | 4 | 4 |
| Normal | 12 | 17 | 3 | 4 | 4 |
| wct\_rcon\_goff | Branch | Common | Feature Name | psi\_group\_change | kmem\_cache\_alloc\_node | perf\_event\_groups\_insert | event\_sched\_in | merge\_sched\_in |
| Attack | 156 | 90 | 73 | 88 | 32 |
| Normal | 75 | 65 | 66 | 73 | 65 |
| Exclusive | Feature Name | kfree | perf\_event\_alloc | memcg\_slab\_free\_hook | rb\_next | visit\_groups\_merge.constprop.0.is |
| Attack | 104 | 71 | 65 | 81 | 73 |
| Normal | 104 | 71 | 65 | 81 | 73 |
| All | Feature Name | kfree | psi\_group\_change | perf\_event\_alloc | kmem\_cache\_alloc\_node | perf\_event\_groups\_insert |
| Attack | 104 | 156 | 71 | 90 | 73 |
| Normal | 104 | 75 | 71 | 65 | 66 |
| Cycles | Common | Feature Name | memset\_erms | perf\_event\_alloc | inherit\_event.constprop.0 | psi\_group\_change | syscall\_exit\_to\_user\_mode |
| Attack | 160 | 155 | 91 | 27 | 66 |
| Normal | 41 | 43 | 92 | 103 | 31 |
| Exclusive | Feature Name | kfree | rb\_next | \_\_\_slab\_alloc | rb\_insert\_color | perf\_event\_update\_userpage |
| Attack | 53 | 77 | 51 | 54 | 55 |
| Normal | 53 | 77 | 51 | 54 | 55 |
| All | Feature Name | memset\_erms | perf\_event\_alloc | inherit\_event.constprop.0 | kfree | psi\_group\_change |
| Attack | 160 | 155 | 91 | 53 | 27 |
| Normal | 41 | 43 | 92 | 53 | 103 |
| Instructions | Common | Feature Name | psi\_group\_change | kfree | perf\_event\_alloc | rb\_next | merge\_sched\_in |
| Attack | 124 | 154 | 72 | 62 | 63 |
| Normal | 143 | 57 | 52 | 13 | 94 |
| Exclusive | Feature Name | memset\_erms | kmem\_cache\_alloc\_node | x86\_pmu\_hw\_config | slab\_free\_freelist\_hook.constprop | x86\_get\_event\_constraints |
| Attack | 85 | 61 | 42 | 50 | 37 |
| Normal | 85 | 61 | 42 | 50 | 37 |
| All | Feature Name | psi\_group\_change | kfree | memset\_erms | perf\_event\_alloc | rb\_next |
| Attack | 124 | 154 | 85 | 72 | 62 |
| Normal | 143 | 57 | 85 | 52 | 13 |
| wct\_rcon\_gon | Branch | Common | Feature Name | psi\_group\_change | x86\_get\_event\_constraints | x86\_pmu\_enable | N/A | N/A |
| Attack | 3 | 3 | 1 | N/A | N/A |
| Normal | 31 | 1 | 1 | N/A | N/A |
| Exclusive | Feature Name | event\_sched\_in | rb\_next | perf\_event\_groups\_first | update\_load\_avg | update\_sg\_wakeup\_stats |
| Attack | 17 | 23 | 1 | 1 | 3 |
| Normal | 17 | 23 | 1 | 1 | 3 |
| All | Feature Name | event\_sched\_in | rb\_next | psi\_group\_change | perf\_event\_groups\_first | update\_load\_avg |
| Attack | 17 | 23 | 3 | 1 | 1 |
| Normal | 17 | 23 | 31 | 1 | 1 |
| Cycles | Common | Feature Name | memset\_erms | native\_write\_msr | N/A | N/A | N/A |
| Attack | 4 | 1 | N/A | N/A | N/A |
| Normal | 8 | 1 | N/A | N/A | N/A |
| Exclusive | Feature Name | psi\_group\_change | merge\_sched\_in | perf\_event\_update\_userpage | syscall\_return\_via\_sysret | perf\_event\_alloc |
| Attack | 24 | 7 | 5 | 5 | 6 |
| Normal | 24 | 7 | 5 | 5 | 6 |
| All | Feature Name | psi\_group\_change | merge\_sched\_in | perf\_event\_update\_userpage | syscall\_return\_via\_sysret | perf\_event\_alloc |
| Attack | 24 | 7 | 5 | 5 | 6 |
| Normal | 24 | 7 | 5 | 5 | 6 |
| Instructions | Common | Feature Name | psi\_group\_change | perf\_event\_alloc | N/A | N/A | N/A |
| Attack | 4 | 2 | N/A | N/A | N/A |
| Normal | 27 | 18 | N/A | N/A | N/A |
| Exclusive | Feature Name | perf\_event\_update\_time | rb\_next | memcg\_slab\_free\_hook | merge\_sched\_in | ctx\_sched\_in |
| Attack | 17 | 19 | 9 | 9 | 5 |
| Normal | 17 | 19 | 9 | 9 | 5 |
| All | Feature Name | perf\_event\_update\_time | rb\_next | memcg\_slab\_free\_hook | psi\_group\_change | merge\_sched\_in |
| Attack | 17 | 19 | 9 | 4 | 9 |
| Normal | 17 | 19 | 9 | 27 | 9 |
| wet\_rcoff\_goff | Branch | Common | Feature Name | psi\_group\_change | perf\_event\_groups\_insert | rb\_next | merge\_sched\_in | memset\_erms |
| Attack | 303 | 254 | 179 | 76 | 135 |
| Normal | 154 | 43 | 58 | 81 | 69 |
| Exclusive | Feature Name | event\_sched\_in | perf\_event\_alloc | kmem\_cache\_alloc\_node\_trace | memcg\_slab\_free\_hook | perf\_iterate\_ctx |
| Attack | 89 | 128 | 96 | 75 | 97 |
| Normal | 89 | 128 | 96 | 75 | 97 |
| All | Feature Name | psi\_group\_change | event\_sched\_in | perf\_event\_alloc | perf\_event\_groups\_insert | kmem\_cache\_alloc\_node\_trace |
| Attack | 303 | 89 | 128 | 254 | 96 |
| Normal | 154 | 89 | 128 | 43 | 96 |
| Cycles | Common | Feature Name | memset\_erms | perf\_event\_alloc | syscall\_exit\_to\_user\_mode | psi\_group\_change | event\_sched\_in |
| Attack | 271 | 186 | 148 | 46 | 66 |
| Normal | 17 | 18 | 62 | 88 | 124 |
| Exclusive | Feature Name | rb\_next | perf\_event\_update\_userpage | perf\_event\_groups\_insert | kfree | kmem\_cache\_alloc\_node\_trace |
| Attack | 137 | 98 | 86 | 87 | 94 |
| Normal | 137 | 98 | 86 | 87 | 94 |
| All | Feature Name | memset\_erms | rb\_next | perf\_event\_alloc | syscall\_exit\_to\_user\_mode | perf\_event\_update\_userpage |
| Attack | 271 | 137 | 186 | 148 | 98 |
| Normal | 17 | 137 | 18 | 62 | 98 |
| Instructions | Common | Feature Name | psi\_group\_change | perf\_event\_alloc | kfree | event\_sched\_in | visit\_groups\_merge.constprop.0.is |
| Attack | 284 | 169 | 214 | 156 | 35 |
| Normal | 133 | 103 | 72 | 48 | 135 |
| Exclusive | Feature Name | perf\_event\_groups\_insert | \_\_srcu\_read\_lock | memset\_erms | x86\_pmu\_event\_init | kmem\_cache\_alloc\_trace |
| Attack | 140 | 106 | 30 | 40 | 59 |
| Normal | 140 | 106 | 30 | 40 | 59 |
| All | Feature Name | psi\_group\_change | perf\_event\_alloc | perf\_event\_groups\_insert | kfree | event\_sched\_in |
| Attack | 284 | 169 | 140 | 214 | 156 |
| Normal | 133 | 103 | 140 | 72 | 48 |
| wet\_rcoff\_gon | Branch | Common | Feature Name | N/A | N/A | N/A | N/A | N/A |
| Attack | N/A | N/A | N/A | N/A | N/A |
| Normal | N/A | N/A | N/A | N/A | N/A |
| Exclusive | Feature Name | psi\_group\_change | merge\_sched\_in | kmem\_cache\_alloc\_node\_trace | kmem\_cache\_alloc\_trace | memset\_erms |
| Attack | 26 | 26 | 24 | 12 | 6 |
| Normal | 26 | 26 | 24 | 12 | 6 |
| All | Feature Name | psi\_group\_change | merge\_sched\_in | kmem\_cache\_alloc\_node\_trace | kmem\_cache\_alloc\_trace | memset\_erms |
| Attack | 26 | 26 | 24 | 12 | 6 |
| Normal | 26 | 26 | 24 | 12 | 6 |
| Cycles | Common | Feature Name | native\_write\_msr | N/A | N/A | N/A | N/A |
| Attack | 1 | N/A | N/A | N/A | N/A |
| Normal | 1 | N/A | N/A | N/A | N/A |
| Exclusive | Feature Name | perf\_event\_alloc | psi\_group\_change | inherit\_event.constprop.0 | syscall\_exit\_to\_user\_mode | memset\_erms |
| Attack | 20 | 4 | 5 | 4 | 5 |
| Normal | 20 | 4 | 5 | 4 | 5 |
| All | Feature Name | perf\_event\_alloc | psi\_group\_change | inherit\_event.constprop.0 | syscall\_exit\_to\_user\_mode | memset\_erms |
| Attack | 20 | 4 | 5 | 4 | 5 |
| Normal | 20 | 4 | 5 | 4 | 5 |
| Instructions | Common | Feature Name | psi\_group\_change | N/A | N/A | N/A | N/A |
| Attack | 24 | N/A | N/A | N/A | N/A |
| Normal | 24 | N/A | N/A | N/A | N/A |
| Exclusive | Feature Name | kfree | event\_sched\_in | perf\_event\_groups\_insert | perf\_event\_alloc | rb\_next |
| Attack | 8 | 20 | 16 | 22 | 6 |
| Normal | 8 | 20 | 16 | 22 | 6 |
| All | Feature Name | kfree | event\_sched\_in | perf\_event\_groups\_insert | perf\_event\_alloc | psi\_group\_change |
| Attack | 8 | 20 | 16 | 22 | 24 |
| Normal | 8 | 20 | 16 | 22 | 24 |
| wet\_rcon\_goff | Branch | Common | Feature Name | psi\_group\_change | event\_sched\_in | kmem\_cache\_alloc\_node\_trace | perf\_event\_update\_userpage | perf\_event\_\_id\_header\_size |
| Attack | 137 | 80 | 69 | 65 | 61 |
| Normal | 124 | 86 | 91 | 82 | 82 |
| Exclusive | Feature Name | kmem\_cache\_alloc\_node | should\_failslab | \_\_update\_load\_avg\_cfs\_rq | perf\_event\_sched\_in | \_\_cgroup\_throttle\_swaprate |
| Attack | 70 | 65 | 60 | 66 | 66 |
| Normal | 70 | 65 | 60 | 66 | 66 |
| All | Feature Name | psi\_group\_change | event\_sched\_in | kmem\_cache\_alloc\_node\_trace | kmem\_cache\_alloc\_node | perf\_event\_update\_userpage |
| Attack | 137 | 80 | 69 | 70 | 65 |
| Normal | 124 | 86 | 91 | 70 | 82 |
| Cycles | Common | Feature Name | memset\_erms | psi\_group\_change | rb\_next | kmem\_cache\_alloc\_node | syscall\_return\_via\_sysret |
| Attack | 157 | 101 | 100 | 88 | 88 |
| Normal | 93 | 128 | 97 | 90 | 87 |
| Exclusive | Feature Name | perf\_event\_update\_userpage | perf\_log\_itrace\_start | account\_event | cgroup\_rstat\_updated | intel\_get\_event\_constraints |
| Attack | 119 | 84 | 84 | 84 | 70 |
| Normal | 119 | 84 | 84 | 84 | 70 |
| All | Feature Name | memset\_erms | perf\_event\_update\_userpage | psi\_group\_change | rb\_next | kmem\_cache\_alloc\_node |
| Attack | 157 | 119 | 101 | 100 | 88 |
| Normal | 93 | 119 | 128 | 97 | 90 |
| Instructions | Common | Feature Name | psi\_group\_change | native\_sched\_clock | kmem\_cache\_alloc\_trace | \_\_srcu\_read\_lock | perf\_event\_groups\_insert |
| Attack | 146 | 96 | 60 | 56 | 43 |
| Normal | 131 | 87 | 87 | 87 | 100 |
| Exclusive | Feature Name | merge\_sched\_in | calc\_timer\_values | cyc2ns\_read\_end | entry\_SYSCALL\_64\_after\_hwframe | kmem\_cache\_alloc\_node |
| Attack | 122 | 123 | 87 | 87 | 76 |
| Normal | 122 | 123 | 87 | 87 | 76 |
| All | Feature Name | psi\_group\_change | merge\_sched\_in | calc\_timer\_values | native\_sched\_clock | cyc2ns\_read\_end |
| Attack | 146 | 122 | 123 | 96 | 87 |
| Normal | 131 | 122 | 123 | 87 | 87 |
| wet\_rcon\_gon | Branch | Common | Feature Name | N/A | N/A | N/A | N/A | N/A |
| Attack | N/A | N/A | N/A | N/A | N/A |
| Normal | N/A | N/A | N/A | N/A | N/A |
| Exclusive | Feature Name | psi\_group\_change | merge\_sched\_in | rb\_next | perf\_event\_groups\_insert | iterate\_groups |
| Attack | 19 | 18 | 17 | 5 | 5 |
| Normal | 19 | 18 | 17 | 5 | 5 |
| All | Feature Name | psi\_group\_change | merge\_sched\_in | rb\_next | perf\_event\_groups\_insert | iterate\_groups |
| Attack | 19 | 18 | 17 | 5 | 5 |
| Normal | 19 | 18 | 17 | 5 | 5 |
| Cycles | Common | Feature Name | perf\_event\_alloc | native\_write\_msr | N/A | N/A | N/A |
| Attack | 3 | 1 | N/A | N/A | N/A |
| Normal | 6 | 1 | N/A | N/A | N/A |
| Exclusive | Feature Name | psi\_group\_change | syscall\_return\_via\_sysret | memset\_erms | visit\_groups\_merge.constprop.0.is | N/A |
| Attack | 17 | 4 | 8 | 3 | N/A |
| Normal | 17 | 4 | 8 | 3 | N/A |
| All | Feature Name | psi\_group\_change | syscall\_return\_via\_sysret | memset\_erms | perf\_event\_alloc | visit\_groups\_merge.constprop.0.is |
| Attack | 17 | 4 | 8 | 3 | 3 |
| Normal | 17 | 4 | 8 | 6 | 3 |
| Instructions | Common | Feature Name | N/A | N/A | N/A | N/A | N/A |
| Attack | N/A | N/A | N/A | N/A | N/A |
| Normal | N/A | N/A | N/A | N/A | N/A |
| Exclusive | Feature Name | psi\_group\_change | event\_sched\_in | kfree | merge\_sched\_in | perf\_event\_groups\_first |
| Attack | 28 | 22 | 5 | 7 | 8 |
| Normal | 28 | 22 | 5 | 7 | 8 |
| All | Feature Name | psi\_group\_change | event\_sched\_in | kfree | merge\_sched\_in | perf\_event\_groups\_first |
| Attack | 28 | 22 | 5 | 7 | 8 |
| Normal | 28 | 22 | 5 | 7 | 8 |
| wid\_rcoff\_goff | Branch | Common | Feature Name | N/A | N/A | N/A | N/A | N/A |
| Attack | N/A | N/A | N/A | N/A | N/A |
| Normal | N/A | N/A | N/A | N/A | N/A |
| Exclusive | Feature Name | psi\_group\_change | kfree | perf\_event\_groups\_insert | merge\_sched\_in | perf\_event\_alloc |
| Attack | 293 | 136 | 119 | 73 | 63 |
| Normal | 293 | 136 | 119 | 73 | 63 |
| All | Feature Name | psi\_group\_change | kfree | perf\_event\_groups\_insert | merge\_sched\_in | perf\_event\_alloc |
| Attack | 293 | 136 | 119 | 73 | 63 |
| Normal | 293 | 136 | 119 | 73 | 63 |
| Cycles | Common | Feature Name | perf\_event\_alloc | psi\_group\_change | N/A | N/A | N/A |
| Attack | 203 | 157 | N/A | N/A | N/A |
| Normal | 53 | 38 | N/A | N/A | N/A |
| Exclusive | Feature Name | memset\_erms | rb\_next | syscall\_exit\_to\_user\_mode | merge\_sched\_in | perf\_event\_update\_userpage |
| Attack | 290 | 144 | 59 | 88 | 119 |
| Normal | 290 | 144 | 59 | 88 | 119 |
| All | Feature Name | memset\_erms | rb\_next | perf\_event\_alloc | syscall\_exit\_to\_user\_mode | merge\_sched\_in |
| Attack | 290 | 144 | 203 | 59 | 88 |
| Normal | 290 | 144 | 53 | 59 | 88 |
| Instructions | Common | Feature Name | N/A | N/A | N/A | N/A | N/A |
| Attack | N/A | N/A | N/A | N/A | N/A |
| Normal | N/A | N/A | N/A | N/A | N/A |
| Exclusive | Feature Name | perf\_event\_alloc | psi\_group\_change | kfree | kmem\_cache\_alloc\_node | perf\_event\_groups\_insert |
| Attack | 285 | 238 | 241 | 138 | 113 |
| Normal | 285 | 238 | 241 | 138 | 113 |
| All | Feature Name | perf\_event\_alloc | psi\_group\_change | kfree | kmem\_cache\_alloc\_node | perf\_event\_groups\_insert |
| Attack | 285 | 238 | 241 | 138 | 113 |
| Normal | 285 | 238 | 241 | 138 | 113 |
|  | Branch | Common | Feature Name | psi\_group\_change | kfree | perf\_event\_groups\_insert | merge\_sched\_in | memset\_erms |
| Attack | 7 | 8 | 1 | 2 | 1 |
| Normal | 28 | 9 | 5 | 21 | 4 |
| Exclusive | Feature Name | event\_sched\_in | inherit\_event.constprop.0 | rb\_insert\_color | native\_sched\_clock | prepare\_task\_switch |
| Attack | 12 | 10 | 7 | 2 | 4 |
| Normal | 12 | 10 | 7 | 2 | 4 |
| All | Feature Name | psi\_group\_change | event\_sched\_in | kfree | perf\_event\_groups\_insert | merge\_sched\_in |
| Attack | 7 | 12 | 8 | 1 | 2 |
| Normal | 28 | 12 | 9 | 5 | 21 |
| Cycles | Common | Feature Name | memset\_erms | native\_write\_msr | N/A | N/A | N/A |
| Attack | 3 | 1 | N/A | N/A | N/A |
| Normal | 24 | 3 | N/A | N/A | N/A |
| Exclusive | Feature Name | perf\_event\_alloc | syscall\_exit\_to\_user\_mode | psi\_group\_change | merge\_sched\_in | rb\_next |
| Attack | 24 | 19 | 15 | 18 | 16 |
| Normal | 24 | 19 | 15 | 18 | 16 |
| All | Feature Name | perf\_event\_alloc | syscall\_exit\_to\_user\_mode | psi\_group\_change | merge\_sched\_in | rb\_next |
| Attack | 24 | 19 | 15 | 18 | 16 |
| Normal | 24 | 19 | 15 | 18 | 16 |
| Instructions | Common | Feature Name | N/A | N/A | N/A | N/A | N/A |
| Attack | N/A | N/A | N/A | N/A | N/A |
| Normal | N/A | N/A | N/A | N/A | N/A |
| Exclusive | Feature Name | psi\_group\_change | perf\_event\_alloc | kfree | kmem\_cache\_alloc\_node\_trace | intel\_cpuc\_finish |
| Attack | 15 | 16 | 13 | 4 | 9 |
| Normal | 15 | 16 | 13 | 4 | 9 |
| All | Feature Name | psi\_group\_change | perf\_event\_alloc | kfree | kmem\_cache\_alloc\_node\_trace | intel\_cpuc\_finish |
| Attack | 15 | 16 | 13 | 4 | 9 |
| Normal | 15 | 16 | 13 | 4 | 9 |
| wid\_rcon\_goff | Branch | Common | Feature Name | psi\_group\_change | perf\_event\_alloc | merge\_sched\_in | inherit\_event.constprop.0 | event\_sched\_in |
| Attack | 158 | 104 | 98 | 108 | 46 |
| Normal | 85 | 81 | 3 | 52 | 8 |
| Exclusive | Feature Name | rb\_next | kmem\_cache\_alloc\_trace | memset\_erms | \_\_perf\_event\_task\_sched\_in | perf\_event\_groups\_first |
| Attack | 99 | 83 | 82 | 69 | 51 |
| Normal | 99 | 83 | 82 | 69 | 51 |
| All | Feature Name | psi\_group\_change | perf\_event\_alloc | rb\_next | merge\_sched\_in | inherit\_event.constprop.0 |
| Attack | 158 | 104 | 99 | 98 | 108 |
| Normal | 85 | 81 | 99 | 3 | 52 |
| Cycles | Common | Feature Name | memset\_erms | perf\_event\_alloc | psi\_group\_change | merge\_sched\_in | syscall\_return\_via\_sysret |
| Attack | 178 | 157 | 70 | 49 | 81 |
| Normal | 8 | 21 | 98 | 99 | 40 |
| Exclusive | Feature Name | inherit\_event.constprop.0 | rb\_next | perf\_iterate\_ctx | \_\_srcu\_read\_lock | \_\_\_slab\_alloc |
| Attack | 133 | 112 | 78 | 38 | 48 |
| Normal | 133 | 112 | 78 | 38 | 48 |
| All | Feature Name | inherit\_event.constprop.0 | rb\_next | memset\_erms | perf\_event\_alloc | psi\_group\_change |
| Attack | 133 | 112 | 178 | 157 | 70 |
| Normal | 133 | 112 | 8 | 21 | 98 |
| Instructions | Common | Feature Name | psi\_group\_change | perf\_event\_alloc | perf\_event\_groups\_insert | kfree | merge\_sched\_in |
| Attack | 180 | 173 | 77 | 96 | 31 |
| Normal | 141 | 63 | 101 | 23 | 34 |
| Exclusive | Feature Name | kmem\_cache\_alloc\_node | rb\_next | inherit\_event.constprop.0 | calc\_timer\_values | x86\_pmu\_hw\_config |
| Attack | 104 | 82 | 80 | 81 | 34 |
| Normal | 104 | 82 | 80 | 81 | 34 |
| All | Feature Name | psi\_group\_change | perf\_event\_alloc | perf\_event\_groups\_insert | kmem\_cache\_alloc\_node | kfree |
| Attack | 180 | 173 | 77 | 104 | 96 |
| Normal | 141 | 63 | 101 | 104 | 23 |
| wid\_rcon\_go | Branch | Common | Feature Name | x86\_pmu\_enable | N/A | N/A | N/A | N/A |
| Attack | 1 | N/A | N/A | N/A | N/A |
| Normal | 1 | N/A | N/A | N/A | N/A |
| Exclusive | Feature Name | psi\_group\_change | merge\_sched\_in | futex\_wake | ctx\_sched\_in | x86\_setup\_perfctr |
| Attack | 31 | 21 | 3 | 6 | 4 |
| Normal | 31 | 21 | 3 | 6 | 4 |
| All | Feature Name | psi\_group\_change | merge\_sched\_in | futex\_wake | ctx\_sched\_in | x86\_setup\_perfctr |
| Attack | 31 | 21 | 3 | 6 | 4 |
| Normal | 31 | 21 | 3 | 6 | 4 |
| Cycles | Common | Feature Name | syscall\_exit\_to\_user\_mode | native\_write\_msr | N/A | N/A | N/A |
| Attack | 1 | 1 | N/A | N/A | N/A |
| Normal | 5 | 1 | N/A | N/A | N/A |
| Exclusive | Feature Name | perf\_event\_update\_userpage | psi\_group\_change | rb\_next | memset\_erms | event\_sched\_in |
| Attack | 31 | 24 | 15 | 2 | 11 |
| Normal | 31 | 24 | 15 | 2 | 11 |
| All | Feature Name | perf\_event\_update\_userpage | psi\_group\_change | rb\_next | memset\_erms | event\_sched\_in |
| Attack | 31 | 24 | 15 | 2 | 11 |
| Normal | 31 | 24 | 15 | 2 | 11 |
| Instructions | Common | Feature Name | kfree | N/A | N/A | N/A | N/A |
| Attack | 3 | N/A | N/A | N/A | N/A |
| Normal | 4 | N/A | N/A | N/A | N/A |
| Exclusive | Feature Name | psi\_group\_change | merge\_sched\_in | perf\_event\_groups\_first | calc\_timer\_values | x86\_get\_event\_constraints |
| Attack | 34 | 22 | 12 | 12 | 2 |
| Normal | 34 | 22 | 12 | 12 | 2 |
| All | Feature Name | psi\_group\_change | merge\_sched\_in | perf\_event\_groups\_first | calc\_timer\_values | x86\_get\_event\_constraints |
| Attack | 34 | 22 | 12 | 12 | 2 |
| Normal | 34 | 22 | 12 | 12 | 2 |

Table 32. Final basic feature sizes of GS under all the attack scenarios

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Scenario | Type 1 | Type 2 | Type 3 | Value | | | | |
| cid\_rcoff\_goff | Branch | Common | Feature Name | psi\_group\_change | merge\_sched\_in | event\_sched\_in | visit\_groups\_merge.constprop.0.is | rb\_next |
| Attack | 359 | 344 | 320 | 253 | 192 |
| Normal | 362 | 356 | 347 | 261 | 236 |
| Exclusive | Feature Name | \_\_cgroup\_bpf\_run\_filter\_skb | timerqueue\_add | kmem\_cache\_free | tcp\_write\_xmit | skb\_release\_data |
| Attack | 99 | 87 | 76 | 74 | 67 |
| Normal | 99 | 87 | 76 | 74 | 67 |
| All | Feature Name | psi\_group\_change | merge\_sched\_in | event\_sched\_in | visit\_groups\_merge.constprop.0.is | rb\_next |
| Attack | 359 | 344 | 320 | 253 | 192 |
| Normal | 362 | 356 | 347 | 261 | 236 |
| Cycles | Common | Feature Name | psi\_group\_change | syscall\_exit\_to\_user\_mode | perf\_event\_update\_userpage | entry\_SYSCALL\_64\_after\_hwframe | perf\_event\_groups\_first |
| Attack | 332 | 273 | 335 | 223 | 297 |
| Normal | 278 | 319 | 234 | 298 | 219 |
| Exclusive | Feature Name | \_\_dev\_queue\_xmit | ip\_finish\_output2 | kfree | \_\_inet\_lookup\_established | schedule\_timeout |
| Attack | 95 | 62 | 38 | 36 | 29 |
| Normal | 95 | 62 | 38 | 36 | 29 |
| All | Feature Name | psi\_group\_change | syscall\_exit\_to\_user\_mode | perf\_event\_update\_userpage | entry\_SYSCALL\_64\_after\_hwframe | perf\_event\_groups\_first |
| Attack | 332 | 273 | 335 | 223 | 297 |
| Normal | 278 | 319 | 234 | 298 | 219 |
| Instructions | Common | Feature Name | psi\_group\_change | merge\_sched\_in | event\_sched\_in | native\_sched\_clock | perf\_event\_update\_userpage |
| Attack | 364 | 318 | 318 | 182 | 158 |
| Normal | 352 | 342 | 339 | 235 | 249 |
| Exclusive | Feature Name | \_\_cgroup\_bpf\_run\_filter\_skb | \_\_dev\_queue\_xmit | do\_poll.constprop.0 | \_\_ip\_queue\_xmit | timerqueue\_add |
| Attack | 167 | 159 | 160 | 82 | 78 |
| Normal | 167 | 159 | 160 | 82 | 78 |
| All | Feature Name | psi\_group\_change | merge\_sched\_in | event\_sched\_in | native\_sched\_clock | perf\_event\_update\_userpage |
| Attack | 364 | 318 | 318 | 182 | 158 |
| Normal | 352 | 342 | 339 | 235 | 249 |
| cid\_rcoff\_gon | Branch | Common | Feature Name | psi\_group\_change | merge\_sched\_in | event\_sched\_in | visit\_groups\_merge.constprop.0.is | rb\_next |
| Attack | 362 | 356 | 347 | 261 | 236 |
| Normal | 36 | 36 | 30 | 20 | 22 |
| Exclusive | Feature Name | do\_poll.constprop.0 | exit\_to\_user\_mode\_loop | timerqueue\_add | update\_cfs\_group | dequeue\_task\_fair |
| Attack | 191 | 93 | 87 | 81 | 80 |
| Normal | 191 | 93 | 87 | 81 | 80 |
| All | Feature Name | do\_poll.constprop.0 | psi\_group\_change | merge\_sched\_in | event\_sched\_in | visit\_groups\_merge.constprop.0.is |
| Attack | 191 | 362 | 356 | 347 | 261 |
| Normal | 191 | 36 | 36 | 30 | 20 |
| Cycles | Common | Feature Name | syscall\_exit\_to\_user\_mode | entry\_SYSCALL\_64\_after\_hwframe | psi\_group\_change | merge\_sched\_in | perf\_event\_update\_userpage |
| Attack | 319 | 298 | 278 | 262 | 234 |
| Normal | 34 | 30 | 33 | 12 | 23 |
| Exclusive | Feature Name | update\_load\_avg | do\_syscall\_64 | arch\_perf\_update\_userpage | \_\_fget\_files | do\_vfs\_ioctl |
| Attack | 137 | 115 | 104 | 97 | 77 |
| Normal | 137 | 115 | 104 | 97 | 77 |
| All | Feature Name | syscall\_exit\_to\_user\_mode | entry\_SYSCALL\_64\_after\_hwframe | psi\_group\_change | update\_load\_avg | merge\_sched\_in |
| Attack | 319 | 298 | 278 | 137 | 262 |
| Normal | 34 | 30 | 33 | 137 | 12 |
| Instructions | Common | Feature Name | psi\_group\_change | merge\_sched\_in | event\_sched\_in | perf\_event\_update\_userpage | native\_sched\_clock |
| Attack | 352 | 342 | 339 | 249 | 235 |
| Normal | 37 | 34 | 34 | 14 | 27 |
| Exclusive | Feature Name | \_\_fget\_files | \_\_update\_load\_avg\_se | calc\_timer\_values | syscall\_return\_via\_sysret | perf\_log\_itrace\_start |
| Attack | 157 | 149 | 73 | 64 | 62 |
| Normal | 157 | 149 | 73 | 64 | 62 |
| All | Feature Name | psi\_group\_change | merge\_sched\_in | event\_sched\_in | \_\_fget\_files | \_\_update\_load\_avg\_se |
| Attack | 352 | 342 | 339 | 157 | 149 |
| Normal | 37 | 34 | 34 | 157 | 149 |
| cid\_rcon\_goff | Branch | Common | Feature Name | psi\_group\_change | event\_sched\_in | merge\_sched\_in | visit\_groups\_merge.constprop.0.is | rb\_next |
| Attack | 193 | 192 | 186 | 164 | 93 |
| Normal | 198 | 196 | 193 | 184 | 133 |
| Exclusive | Feature Name | tcp\_recvmsg\_locked | \_\_dev\_queue\_xmit | sock\_poll | \_\_mod\_timer | aa\_profile\_af\_perm |
| Attack | 44 | 42 | 40 | 36 | 28 |
| Normal | 44 | 42 | 40 | 36 | 28 |
| All | Feature Name | psi\_group\_change | event\_sched\_in | merge\_sched\_in | visit\_groups\_merge.constprop.0.is | rb\_next |
| Attack | 193 | 192 | 186 | 164 | 93 |
| Normal | 198 | 196 | 193 | 184 | 133 |
| Cycles | Common | Feature Name | perf\_event\_update\_userpage | merge\_sched\_in | syscall\_exit\_to\_user\_mode | psi\_group\_change | visit\_groups\_merge.constprop.0.is |
| Attack | 183 | 167 | 154 | 171 | 151 |
| Normal | 151 | 154 | 159 | 122 | 85 |
| Exclusive | Feature Name | \_\_x64\_sys\_poll | tcp\_sendmsg\_locked | kfree | tcp\_event\_data\_recv | task\_clock\_event\_add |
| Attack | 53 | 42 | 19 | 19 | 21 |
| Normal | 53 | 42 | 19 | 19 | 21 |
| All | Feature Name | perf\_event\_update\_userpage | merge\_sched\_in | syscall\_exit\_to\_user\_mode | psi\_group\_change | visit\_groups\_merge.constprop.0.is |
| Attack | 183 | 167 | 154 | 171 | 151 |
| Normal | 151 | 154 | 159 | 122 | 85 |
| Instructions | Common | Feature Name | psi\_group\_change | event\_sched\_in | merge\_sched\_in | native\_sched\_clock | perf\_swevent\_add |
| Attack | 193 | 178 | 173 | 113 | 132 |
| Normal | 199 | 196 | 149 | 130 | 105 |
| Exclusive | Feature Name | tcp\_ack | tcp\_write\_xmit | tcp\_v4\_rcv | tcp\_sendmsg\_locked | aa\_label\_sk\_perm.part.0 |
| Attack | 59 | 56 | 51 | 41 | 32 |
| Normal | 59 | 56 | 51 | 41 | 32 |
| All | Feature Name | psi\_group\_change | event\_sched\_in | merge\_sched\_in | native\_sched\_clock | perf\_swevent\_add |
| Attack | 193 | 178 | 173 | 113 | 132 |
| Normal | 199 | 196 | 149 | 130 | 105 |
| cid\_rcon\_gon | Branch | Common | Feature Name | psi\_group\_change | event\_sched\_in | perf\_event\_update\_userpage | merge\_sched\_in | arch\_perf\_update\_userpage |
| Attack | 12 | 12 | 8 | 10 | 8 |
| Normal | 32 | 29 | 26 | 21 | 20 |
| Exclusive | Feature Name | \_\_update\_load\_avg\_se | \_raw\_spin\_lock | \_\_schedule | native\_sched\_clock | perf\_log\_itrace\_start |
| Attack | 29 | 12 | 22 | 21 | 11 |
| Normal | 29 | 12 | 22 | 21 | 11 |
| All | Feature Name | \_\_update\_load\_avg\_se | psi\_group\_change | event\_sched\_in | \_raw\_spin\_lock | \_\_schedule |
| Attack | 29 | 12 | 12 | 12 | 22 |
| Normal | 29 | 32 | 29 | 12 | 22 |
| Cycles | Common | Feature Name | merge\_sched\_in | psi\_group\_change | rb\_next | syscall\_return\_via\_sysret | syscall\_exit\_to\_user\_mode |
| Attack | 10 | 11 | 10 | 10 | 10 |
| Normal | 34 | 32 | 32 | 31 | 30 |
| Exclusive | Feature Name | entry\_SYSCALL\_64\_after\_hwframe | native\_sched\_clock | copy\_user\_enhanced\_fast\_string | \_raw\_spin\_lock | raw\_local\_deliver |
| Attack | 36 | 34 | 9 | 7 | 7 |
| Normal | 36 | 34 | 9 | 7 | 7 |
| All | Feature Name | entry\_SYSCALL\_64\_after\_hwframe | native\_sched\_clock | merge\_sched\_in | psi\_group\_change | rb\_next |
| Attack | 36 | 34 | 10 | 11 | 10 |
| Normal | 36 | 34 | 34 | 32 | 32 |
| Instructions | Common | Feature Name | psi\_group\_change | perf\_event\_update\_userpage | arch\_perf\_update\_userpage | merge\_sched\_in | skb\_release\_data |
| Attack | 7 | 6 | 1 | 6 | 6 |
| Normal | 38 | 35 | 32 | 22 | 21 |
| Exclusive | Feature Name | rb\_next | event\_sched\_in | iterate\_groups | \_\_update\_load\_avg\_se | visit\_groups\_merge.constprop.0.is |
| Attack | 37 | 35 | 30 | 29 | 27 |
| Normal | 37 | 35 | 30 | 29 | 27 |
| All | Feature Name | rb\_next | event\_sched\_in | iterate\_groups | \_\_update\_load\_avg\_se | visit\_groups\_merge.constprop.0.is |
| Attack | 37 | 35 | 30 | 29 | 27 |
| Normal | 37 | 35 | 30 | 29 | 27 |
| wct\_rcoff\_goff | Branch | Common | Feature Name | psi\_group\_change | merge\_sched\_in | event\_sched\_in | visit\_groups\_merge.constprop.0.is | rb\_next |
| Attack | 355 | 352 | 338 | 285 | 222 |
| Normal | 344 | 344 | 320 | 270 | 200 |
| Exclusive | Feature Name | \_\_tcp\_transmit\_skb | tcp\_clean\_rtx\_queue.constprop.0 | do\_poll.constprop.0 | sock\_poll | \_\_netif\_receive\_skb\_core |
| Attack | 213 | 193 | 150 | 120 | 87 |
| Normal | 213 | 193 | 150 | 120 | 87 |
| All | Feature Name | psi\_group\_change | merge\_sched\_in | event\_sched\_in | visit\_groups\_merge.constprop.0.is | \_\_tcp\_transmit\_skb |
| Attack | 355 | 352 | 328 | 285 | 213 |
| Normal | 344 | 344 | 320 | 270 | 213 |
| Cycles | Common | Feature Name | psi\_group\_change | merge\_sched\_in | syscall\_exit\_to\_user\_mode | perf\_event\_update\_userpage | entry\_SYSCALL\_64\_after\_hwframe |
| Attack | 344 | 337 | 312 | 359 | 247 |
| Normal | 327 | 295 | 319 | 227 | 242 |
| Exclusive | Feature Name | do\_sys\_poll | tcp\_sendmsg\_locked | tcp\_rcv\_established | \_\_netif\_receive\_skb\_core.constpro | aa\_sk\_perm |
| Attack | 123 | 108 | 87 | 77 | 73 |
| Normal | 123 | 108 | 87 | 77 | 73 |
| All | Feature Name | psi\_group\_change | merge\_sched\_in | syscall\_exit\_to\_user\_mode | perf\_event\_update\_userpage | entry\_SYSCALL\_64\_after\_hwframe |
| Attack | 344 | 337 | 312 | 359 | 247 |
| Normal | 327 | 295 | 319 | 227 | 242 |
| Instructions | Common | Feature Name | psi\_group\_change | merge\_sched\_in | event\_sched\_in | native\_sched\_clock | 'visit\_groups\_merge.constprop.0.is |
| Attack | 361 | 298 | 315 | 215 | 186 |
| Normal | 355 | 320 | 244 | 261 | 208 |
| Exclusive | Feature Name | ip\_rcv\_core | \_\_ip\_queue\_xmit | \_\_netif\_receive\_skb\_core.constpro | tcp\_sendmsg\_locked | tcp\_v4\_rcv |
| Attack | 103 | 94 | 81 | 79 | 77 |
| Normal | 103 | 94 | 81 | 79 | 77 |
| All | Feature Name | psi\_group\_change | merge\_sched\_in | event\_sched\_in | native\_sched\_clock | visit\_groups\_merge.constprop.0.is |
| Attack | 361 | 298 | 315 | 215 | 186 |
| Normal | 355 | 320 | 244 | 261 | 208 |
| wct\_rcoff\_gon | Branch | Common | Feature Name | psi\_group\_change | merge\_sched\_in | event\_sched\_in | rb\_next | tcp\_write\_xmit |
| Attack | 13 | 10 | 4 | 9 | 10 |
| Normal | 38 | 36 | 33 | 23 | 14 |
| Exclusive | Feature Name | \_\_netif\_receive\_skb\_core.constpro | loopback\_xmit | \_\_softirqentry\_text\_start | tcp\_clean\_rtx\_queue.constprop.0 | tcp\_rearm\_rto |
| Attack | 27 | 21 | 20 | 20 | 18 |
| Normal | 27 | 21 | 20 | 20 | 18 |
| All | Feature Name | psi\_group\_change | merge\_sched\_in | \_\_netif\_receive\_skb\_core.constpro | loopback\_xmit | event\_sched\_in |
| Attack | 13 | 10 | 27 | 21 | 4 |
| Normal | 38 | 36 | 27 | 21 | 33 |
| Cycles | Common | Feature Name | perf\_event\_update\_userpage | psi\_group\_change | rb\_next | syscall\_exit\_to\_user\_mode | merge\_sched\_in |
| Attack | 10 | 7 | 10 | 5 | 7 |
| Normal | 33 | 33 | 26 | 33 | 28 |
| Exclusive | Feature Name | do\_poll.constprop.0 | syscall\_return\_via\_sysret | event\_sched\_in | \_\_calc\_delta | \_\_entry\_text\_start |
| Attack | 30 | 27 | 20 | 16 | 15 |
| Normal | 30 | 27 | 20 | 16 | 15 |
| All | Feature Name | do\_poll.constprop.0 | syscall\_return\_via\_sysret | perf\_event\_update\_userpage | psi\_group\_change | rb\_next |
| Attack | 30 | 27 | 10 | 7 | 10 |
| Normal | 30 | 27 | 33 | 33 | 26 |
| Instructions | Common | Feature Name | psi\_group\_change | event\_sched\_in | perf\_event\_update\_userpage | merge\_sched\_in | native\_sched\_clock |
| Attack | 7 | 7 | 2 | 12 | 5 |
| Normal | 38 | 31 | 33 | 11 | 23 |
| Exclusive | Feature Name | sched\_clock\_cpu | reweight\_entity | aa\_label\_next\_confined | perf\_event\_update\_time | update\_curr |
| Attack | 35 | 25 | 21 | 21 | 20 |
| Normal | 35 | 25 | 21 | 21 | 20 |
| All | Feature Name | sched\_clock\_cpu | psi\_group\_change | reweight\_entity | event\_sched\_in | aa\_label\_next\_confined |
| Attack | 35 | 7 | 25 | 7 | 21 |
| Normal | 35 | 38 | 25 | 31 | 21 |
| wct\_rcon\_goff | Branch | Common | Feature Name | psi\_group\_change | event\_sched\_in | merge\_sched\_in | visit\_groups\_merge.constprop.0.is | rb\_next |
| Attack | 183 | 166 | 177 | 165 | 153 |
| Normal | 184 | 183 | 159 | 134 | 127 |
| Exclusive | Feature Name | do\_poll.constprop.0 | \_\_tcp\_transmit\_skb | do\_sys\_poll | tcp\_ack | \_\_virt\_addr\_valid |
| Attack | 118 | 77 | 82 | 73 | 62 |
| Normal | 118 | 77 | 82 | 73 | 62 |
| All | Feature Name | psi\_group\_change | event\_sched\_in | merge\_sched\_in | visit\_groups\_merge.constprop.0.is | rb\_next |
| Attack | 183 | 166 | 177 | 165 | 153 |
| Normal | 184 | 183 | 159 | 134 | 127 |
| Cycles | Common | Feature Name | perf\_event\_update\_userpage | psi\_group\_change | syscall\_exit\_to\_user\_mode | merge\_sched\_in | rb\_next |
| Attack | 173 | 170 | 144 | 154 | 159 |
| Normal | 183 | 163 | 181 | 130 | 118 |
| Exclusive | Feature Name | do\_poll.constprop.0 | tcp\_write\_xmit | \_\_x64\_sys\_poll | sock\_poll | select\_estimate\_accuracy |
| Attack | 70 | 35 | 32 | 28 | 27 |
| Normal | 70 | 35 | 32 | 28 | 27 |
| All | Feature Name | perf\_event\_update\_userpage | psi\_group\_change | syscall\_exit\_to\_user\_mode | merge\_sched\_in | rb\_next |
| Attack | 173 | 170 | 144 | 154 | 159 |
| Normal | 183 | 163 | 181 | 130 | 118 |
| Instructions | Common | Feature Name | psi\_group\_change | merge\_sched\_in | event\_sched\_in | native\_sched\_clock | arch\_perf\_update\_userpage |
| Attack | 183 | 174 | 154 | 142 | 151 |
| Normal | 189 | 179 | 160 | 151 | 128 |
| Exclusive | Feature Name | do\_poll.constprop.0 | \_\_dev\_queue\_xmit | tcp\_clean\_rtx\_queue.constprop.0 | memcg\_slab\_free\_hook | do\_sys\_poll |
| Attack | 64 | 46 | 44 | 33 | 36 |
| Normal | 64 | 46 | 44 | 33 | 36 |
| All | Feature Name | psi\_group\_change | merge\_sched\_in | event\_sched\_in | native\_sched\_clock | arch\_perf\_update\_userpage |
| Attack | 183 | 174 | 154 | 142 | 151 |
| Normal | 189 | 179 | 160 | 151 | 128 |
| wct\_rcon\_gon | Branch | Common | Feature Name | merge\_sched\_in | psi\_group\_change | event\_sched\_in | visit\_groups\_merge.constprop.0.is | \_\_tcp\_transmit\_skb |
| Attack | 12 | 12 | 11 | 11 | 9 |
| Normal | 33 | 33 | 28 | 28 | 31 |
| Exclusive | Feature Name | sk\_stream\_alloc\_skb | rcu\_read\_unlock\_strict | perf\_swevent\_add | timerqueue\_add | migrate\_disable |
| Attack | 29 | 24 | 21 | 20 | 20 |
| Normal | 29 | 24 | 21 | 20 | 20 |
| All | Feature Name | sk\_stream\_alloc\_skb | merge\_sched\_in | psi\_group\_change | event\_sched\_in | visit\_groups\_merge.constprop.0.is |
| Attack | 29 | 12 | 12 | 11 | 11 |
| Normal | 29 | 33 | 33 | 28 | 28 |
| Cycles | Common | Feature Name | perf\_event\_groups\_first | psi\_group\_change | syscall\_exit\_to\_user\_mode | perf\_swevent\_add | perf\_event\_update\_userpage |
| Attack | 9 | 9 | 8 | 7 | 8 |
| Normal | 26 | 24 | 25 | 26 | 18 |
| Exclusive | Feature Name | merge\_sched\_in | rb\_next | kmem\_cache\_alloc\_node | exit\_to\_user\_mode\_prepare | inet\_recvmsg |
| Attack | 33 | 26 | 18 | 15 | 14 |
| Normal | 33 | 26 | 18 | 15 | 14 |
| All | Feature Name | merge\_sched\_in | rb\_next | perf\_event\_groups\_first | psi\_group\_change | syscall\_exit\_to\_user\_mode |
| Attack | 33 | 26 | 9 | 9 | 8 |
| Normal | 33 | 26 | 26 | 24 | 25 |
| Instructions | Common | Feature Name | merge\_sched\_in | psi\_group\_change | native\_sched\_clock | perf\_event\_update\_userpage | tcp\_clean\_rtx\_queue.constprop.0 |
| Attack | 10 | 8 | 9 | 7 | 7 |
| Normal | 34 | 37 | 29 | 32 | 27 |
| Exclusive | Feature Name | arch\_perf\_update\_userpage | \_\_tcp\_transmit\_skb | \_\_alloc\_skb | perf\_swevent\_add | perf\_event\_update\_time |
| Attack | 27 | 25 | 25 | 24 | 22 |
| Normal | 27 | 25 | 25 | 24 | 22 |
| All | Feature Name | arch\_perf\_update\_userpage | merge\_sched\_in | psi\_group\_change | \_\_tcp\_transmit\_skb | \_\_alloc\_skb |
| Attack | 27 | 10 | 8 | 25 | 25 |
| Normal | 27 | 34 | 37 | 25 | 25 |
| wet\_rcoff\_goff | Branch | Common | Feature Name | psi\_group\_change | merge\_sched\_in | event\_sched\_in | visit\_groups\_merge.constprop.0.is | arch\_perf\_update\_userpage |
| Attack | 330 | 316 | 255 | 287 | 246 |
| Normal | 334 | 311 | 297 | 237 | 132 |
| Exclusive | Feature Name | hrtimer\_start\_range\_ns | tcp\_clean\_rtx\_queue.constprop.0 | \_\_kmalloc\_node\_track\_caller | \_\_sys\_sendto | ipv4\_dst\_check |
| Attack | 54 | 54 | 45 | 42 | 42 |
| Normal | 54 | 54 | 45 | 42 | 42 |
| All | Feature Name | psi\_group\_change | merge\_sched\_in | event\_sched\_in | visit\_groups\_merge.constprop.0.is | arch\_perf\_update\_userpage |
| Attack | 330 | 316 | 255 | 287 | 246 |
| Normal | 334 | 311 | 297 | 237 | 132 |
| Cycles | Common | Feature Name | merge\_sched\_in | syscall\_exit\_to\_user\_mode | perf\_event\_update\_userpage | psi\_group\_change | event\_sched\_in |
| Attack | 248 | 197 | 264 | 176 | 208 |
| Normal | 255 | 283 | 211 | 299 | 239 |
| Exclusive | Feature Name | \_\_rseq\_handle\_notify\_resume | clear\_buddies | do\_syscall\_64 | ktime\_get\_ts64 | \_\_local\_bh\_enable\_ip |
| Attack | 109 | 91 | 84 | 57 | 41 |
| Normal | 109 | 91 | 84 | 57 | 41 |
| All | Feature Name | merge\_sched\_in | syscall\_exit\_to\_user\_mode | perf\_event\_update\_userpage | psi\_group\_change | event\_sched\_in |
| Attack | 248 | 197 | 264 | 176 | 208 |
| Normal | 255 | 283 | 211 | 299 | 239 |
| Instructions | Common | Feature Name | psi\_group\_change | event\_sched\_in | merge\_sched\_in | visit\_groups\_merge.constprop.0.is | perf\_event\_update\_userpage |
| Attack | 324 | 316 | 243 | 237 | 214 |
| Normal | 338 | 328 | 282 | 247 | 251 |
| Exclusive | Feature Name | \_\_tcp\_transmit\_skb | dequeue\_task | \_\_x64\_sys\_poll | \_\_alloc\_skb | \_\_put\_user\_nocheck\_8 |
| Attack | 96 | 60 | 51 | 51 | 47 |
| Normal | 96 | 60 | 51 | 51 | 47 |
| All | Feature Name | psi\_group\_change | event\_sched\_in | merge\_sched\_in | visit\_groups\_merge.constprop.0.is | perf\_event\_update\_userpage |
| Attack | 324 | 316 | 243 | 237 | 214 |
| Normal | 338 | 328 | 282 | 247 | 251 |
| wet\_rcoff\_gon | Branch | Common | Feature Name | merge\_sched\_in | psi\_group\_change | event\_sched\_in | iterate\_groups | visit\_groups\_merge.constprop.0.is |
| Attack | 11 | 11 | 11 | 7 | 8 |
| Normal | 32 | 32 | 29 | 25 | 19 |
| Exclusive | Feature Name | native\_sched\_clock | tcp\_recvmsg\_locked | tcp\_sendmsg\_locked | \_\_build\_skb\_around | tcp\_release\_cb |
| Attack | 29 | 28 | 23 | 19 | 18 |
| Normal | 29 | 28 | 23 | 19 | 18 |
| All | Feature Name | native\_sched\_clock | tcp\_recvmsg\_locked | merge\_sched\_in | psi\_group\_change | event\_sched\_in |
| Attack | 29 | 28 | 11 | 11 | 11 |
| Normal | 29 | 28 | 32 | 32 | 29 |
| Cycles | Common | Feature Name | psi\_group\_change | rb\_next | \_\_fget\_files | \_\_perf\_event\_task\_sched\_in | syscall\_exit\_to\_user\_mode |
| Attack | 9 | 7 | 8 | 4 | 2 |
| Normal | 33 | 33 | 28 | 32 | 34 |
| Exclusive | Feature Name | event\_sched\_in | do\_sys\_poll | tcp\_chrono\_stop | skb\_page\_frag\_refill | exit\_to\_user\_mode\_loop |
| Attack | 33 | 27 | 9 | 15 | 8 |
| Normal | 33 | 27 | 9 | 15 | 8 |
| All | Feature Name | event\_sched\_in | do\_sys\_poll | psi\_group\_change | rb\_next | \_\_fget\_files |
| Attack | 33 | 27 | 9 | 7 | 8 |
| Normal | 33 | 27 | 33 | 33 | 28 |
| Instructions | Common | Feature Name | merge\_sched\_in | psi\_group\_change | visit\_groups\_merge.constprop.0.is | \_\_update\_load\_avg\_se | rb\_next |
| Attack | 12 | 12 | 11 | 6 | 2 |
| Normal | 38 | 38 | 27 | 31 | 29 |
| Exclusive | Feature Name | \_\_netif\_receive\_skb\_core.constpro | \_\_tcp\_transmit\_skb | ip\_rcv\_core | \_\_inet\_lookup\_established | \_\_cgroup\_bpf\_run\_filter\_skb |
| Attack | 28 | 28 | 12 | 12 | 20 |
| Normal | 28 | 28 | 12 | 12 | 20 |
| All | Feature Name | merge\_sched\_in | psi\_group\_change | \_\_netif\_receive\_skb\_core | \_\_tcp\_transmit\_skb | visit\_groups\_merge.constprop.0.is |
| Attack | 12 | 12 | 28 | 28 | 11 |
| Normal | 38 | 38 | 28 | 28 | 27 |
| wet\_rcon\_goff | Branch | Common | Feature Name | psi\_group\_change | event\_sched\_in | merge\_sched\_in | visit\_groups\_merge.constprop.0.is | do\_poll.constprop.0 |
| Attack | 167 | 166 | 164 | 157 | 105 |
| Normal | 175 | 165 | 161 | 109 | 90 |
| Exclusive | Feature Name | \_\_get\_user\_8 | tcp\_current\_mss | \_\_x64\_sys\_futex | \_\_ksize | ip\_queue\_xmit |
| Attack | 48 | 39 | 38 | 37 | 37 |
| Normal | 48 | 39 | 38 | 37 | 37 |
| All | Feature Name | psi\_group\_change | event\_sched\_in | merge\_sched\_in | 'visit\_groups\_merge.constprop.0.is | do\_poll.constprop.0 |
| Attack | 167 | 166 | 164 | 157 | 105 |
| Normal | 175 | 165 | 161 | 109 | 90 |
| Cycles | Common | Feature Name | psi\_group\_change | perf\_event\_update\_userpage | syscall\_exit\_to\_user\_mode | merge\_sched\_in | visit\_groups\_merge.constprop.0.is |
| Attack | 154 | 144 | 149 | 84 | 89 |
| Normal | 145 | 153 | 124 | 144 | 126 |
| Exclusive | Feature Name | \_\_update\_load\_avg\_cfs\_rq | \_\_rseq\_handle\_notify\_resume | rb\_insert\_color | \_\_calc\_delta | remove\_wait\_queue |
| Attack | 39 | 31 | 31 | 31 | 25 |
| Normal | 39 | 31 | 31 | 31 | 25 |
| All | Feature Name | psi\_group\_change | perf\_event\_update\_userpage | syscall\_exit\_to\_user\_mode | merge\_sched\_in | visit\_groups\_merge.constprop.0.is |
| Attack | 154 | 144 | 149 | 84 | 89 |
| Normal | 145 | 153 | 124 | 144 | 126 |
| Instructions | Common | Feature Name | psi\_group\_change | event\_sched\_in | perf\_swevent\_add | native\_sched\_clock | merge\_sched\_in |
| Attack | 167 | 164 | 150 | 138 | 138 |
| Normal | 179 | 157 | 127 | 132 | 122 |
| Exclusive | Feature Name | \_\_inet\_lookup\_established | tcp\_v4\_inbound\_md5\_hash | \_\_cgroup\_bpf\_run\_filter\_skb | \_\_tcp\_transmit\_skb | tcp\_ack |
| Attack | 53 | 45 | 38 | 38 | 32 |
| Normal | 53 | 45 | 38 | 38 | 32 |
| All | Feature Name | psi\_group\_change | event\_sched\_in | perf\_swevent\_add | native\_sched\_clock | merge\_sched\_in |
| Attack | 167 | 164 | 150 | 138 | 138 |
| Normal | 179 | 157 | 127 | 132 | 122 |
| wet\_rcon\_gon | Branch | Common | Feature Name | psi\_group\_change | merge\_sched\_in | native\_sched\_clock | event\_sched\_in | rb\_next |
| Attack | 12 | 7 | 9 | 8 | 8 |
| Normal | 34 | 37 | 21 | 18 | 14 |
| Exclusive | Feature Name | perf\_log\_itrace\_start | arch\_perf\_update\_userpage | psi\_task\_switch | reweight\_entity | \_\_update\_load\_avg\_cfs\_rq |
| Attack | 33 | 32 | 24 | 23 | 22 |
| Normal | 33 | 32 | 24 | 23 | 22 |
| All | Feature Name | perf\_log\_itrace\_start | arch\_perf\_update\_userpage | psi\_group\_change | merge\_sched\_in | psi\_task\_switch |
| Attack | 33 | 32 | 12 | 7 | 24 |
| Normal | 33 | 32 | 34 | 37 | 24 |
| Cycles | Common | Feature Name | psi\_group\_change | merge\_sched\_in | \_\_perf\_event\_task\_sched\_in | native\_write\_msr | \_\_virt\_addr\_valid |
| Attack | 6 | 7 | 2 | 4 | 6 |
| Normal | 30 | 27 | 30 | 25 | 10 |
| Exclusive | Feature Name | event\_sched\_in | syscall\_exit\_to\_user\_mode | rb\_next | entry\_SYSCALL\_64\_after\_hwframe | perf\_pmu\_nop\_int |
| Attack | 31 | 29 | 26 | 26 | 19 |
| Normal | 31 | 29 | 26 | 26 | 19 |
| All | Feature Name | event\_sched\_in | syscall\_exit\_to\_user\_mode | rb\_next | entry\_SYSCALL\_64\_after\_hwframe | psi\_group\_change |
| Attack | 31 | 29 | 26 | 26 | 6 |
| Normal | 31 | 29 | 26 | 26 | 30 |
| Instructions | Common | Feature Name | psi\_group\_change | event\_sched\_in | visit\_groups\_merge.constprop.0.is | perf\_event\_update\_userpage | arch\_perf\_update\_userpage |
| Attack | 11 | 11 | 4 | 6 | 8 |
| Normal | 37 | 36 | 31 | 26 | 20 |
| Exclusive | Feature Name | merge\_sched\_in | \_raw\_spin\_lock | ctx\_sched\_in | tcp\_ack | iterate\_groups |
| Attack | 32 | 31 | 27 | 25 | 21 |
| Normal | 32 | 31 | 27 | 25 | 21 |
| All | Feature Name | merge\_sched\_in | \_raw\_spin\_lock | psi\_group\_change | event\_sched\_in | ctx\_sched\_in |
| Attack | 32 | 31 | 11 | 11 | 27 |
| Normal | 32 | 31 | 37 | 36 | 27 |
| wid\_rcoff\_goff | Branch | Common | Feature Name | psi\_group\_change | merge\_sched\_in | event\_sched\_in | visit\_groups\_merge.constprop.0.is | arch\_perf\_update\_userpage |
| Attack | 360 | 359 | 337 | 277 | 199 |
| Normal | 354 | 343 | 344 | 309 | 214 |
| Exclusive | Feature Name | tcp\_clean\_rtx\_queue.constprop.0 | tcp\_ack | \_\_cgroup\_bpf\_run\_filter\_skb | kmem\_cache\_alloc\_node | sk\_stream\_alloc\_skb |
| Attack | 176 | 150 | 76 | 57 | 53 |
| Normal | 176 | 150 | 76 | 57 | 53 |
| All | Feature Name | psi\_group\_change | merge\_sched\_in | event\_sched\_in | visit\_groups\_merge.constprop.0.is | arch\_perf\_update\_userpage |
| Attack | 360 | 359 | 337 | 277 | 199 |
| Normal | 354 | 343 | 344 | 309 | 214 |
| Cycles | Common | Feature Name | syscall\_exit\_to\_user\_mode | psi\_group\_change | merge\_sched\_in | perf\_event\_update\_userpage | rb\_next |
| Attack | 313 | 325 | 269 | 344 | 298 |
| Normal | 324 | 290 | 318 | 215 | 198 |
| Exclusive | Feature Name | aa\_sk\_perm | \_\_ip\_queue\_xmit | do\_vfs\_ioctl | sched\_clock\_cpu | acpi\_os\_read\_port |
| Attack | 87 | 72 | 69 | 58 | 47 |
| Normal | 87 | 72 | 69 | 58 | 47 |
| All | Feature Name | syscall\_exit\_to\_user\_mode | psi\_group\_change | merge\_sched\_in | perf\_event\_update\_userpage | rb\_next |
| Attack | 313 | 325 | 269 | 344 | 298 |
| Normal | 324 | 290 | 318 | 215 | 198 |
| Instructions | Common | Feature Name | psi\_group\_change | event\_sched\_in | merge\_sched\_in | arch\_perf\_update\_userpage | native\_sched\_clock |
| Attack | 354 | 311 | 319 | 158 | 170 |
| Normal | 350 | 348 | 335 | 254 | 233 |
| Exclusive | Feature Name | tcp\_clean\_rtx\_queue.constprop.0 | \_\_cgroup\_bpf\_run\_filter\_skb | \_\_ip\_queue\_xmit | tcp\_v4\_rcv | tcp\_write\_xmit |
| Attack | 174 | 171 | 159 | 143 | 121 |
| Normal | 174 | 171 | 159 | 143 | 121 |
| All | Feature Name | psi\_group\_change | event\_sched\_in | merge\_sched\_in | arch\_perf\_update\_userpage | native\_sched\_clock |
| Attack | 354 | 311 | 319 | 158 | 170 |
| Normal | 350 | 348 | 335 | 254 | 233 |
| wid\_rcoff\_gon | Branch | Common | Feature Name | psi\_group\_change | perf\_event\_groups\_first | merge\_sched\_in | native\_sched\_clock | \_\_update\_load\_avg\_cfs\_rq |
| Attack | 9 | 5 | 2 | 8 | 5 |
| Normal | 35 | 22 | 27 | 14 | 19 |
| Exclusive | Feature Name | arch\_perf\_update\_userpage | tcp\_schedule\_loss\_probe.part.0 | event\_sched\_in | tcp\_v4\_do\_rcv | prepare\_task\_switch |
| Attack | 27 | 26 | 25 | 9 | 9 |
| Normal | 27 | 26 | 25 | 9 | 9 |
| All | Feature Name | arch\_perf\_update\_userpage | tcp\_schedule\_loss\_probe.part.0 | psi\_group\_change | event\_sched\_in | tcp\_v4\_do\_rcv |
| Attack | 27 | 26 | 9 | 25 | 9 |
| Normal | 27 | 26 | 35 | 25 | 9 |
| Cycles | Common | Feature Name | perf\_event\_groups\_first | perf\_event\_update\_userpage | syscall\_exit\_to\_user\_mode | psi\_group\_change | rb\_next |
| Attack | 7 | 7 | 9 | 2 | 8 |
| Normal | 32 | 30 | 25 | 36 | 23 |
| Exclusive | Feature Name | event\_sched\_in | \_\_fget\_files | merge\_sched\_in | \_\_kmalloc\_node\_track\_caller | enqueue\_entity |
| Attack | 35 | 25 | 23 | 23 | 8 |
| Normal | 35 | 25 | 23 | 23 | 8 |
| All | Feature Name | event\_sched\_in | \_\_fget\_files | merge\_sched\_in | \_\_kmalloc\_node\_track\_caller | perf\_event\_groups\_first |
| Attack | 35 | 25 | 23 | 23 | 7 |
| Normal | 35 | 25 | 23 | 23 | 32 |
| Instructions | Common | Feature Name | psi\_group\_change | merge\_sched\_in | visit\_groups\_merge.constprop.0.is | event\_sched\_in | update\_load\_avg |
| Attack | 11 | 10 | 9 | 7 | 2 |
| Normal | 37 | 37 | 34 | 33 | 35 |
| Exclusive | Feature Name | skb\_release\_data | \_\_tcp\_transmit\_skb | rb\_next | \_\_cgroup\_bpf\_run\_filter\_skb | kfence\_ksize |
| Attack | 36 | 34 | 31 | 29 | 25 |
| Normal | 36 | 34 | 31 | 29 | 25 |
| All | Feature Name | skb\_release\_data | \_\_tcp\_transmit\_skb | rb\_next | \_\_cgroup\_bpf\_run\_filter\_skb | psi\_group\_change |
| Attack | 36 | 34 | 31 | 29 | 11 |
| Normal | 36 | 34 | 31 | 29 | 37 |
| wid\_rcon\_goff | Branch | Common | Feature Name | psi\_group\_change | event\_sched\_in | merge\_sched\_in | visit\_groups\_merge.constprop.0.is | perf\_swevent\_add |
| Attack | 197 | 183 | 161 | 133 | 127 |
| Normal | 209 | 191 | 180 | 175 | 114 |
| Exclusive | Feature Name | tcp\_recvmsg\_locked | tcp\_sendmsg\_locked | aa\_profile\_af\_perm | sk\_stream\_alloc\_skb | \_\_mod\_timer |
| Attack | 58 | 55 | 53 | 50 | 46 |
| Normal | 58 | 55 | 53 | 50 | 46 |
| All | Feature Name | psi\_group\_change | event\_sched\_in | merge\_sched\_in | visit\_groups\_merge.constprop.0.is | perf\_swevent\_add |
| Attack | 197 | 183 | 161 | 133 | 127 |
| Normal | 209 | 191 | 180 | 175 | 114 |
| Cycles | Common | Feature Name | psi\_group\_change | perf\_event\_update\_userpage | merge\_sched\_in | rb\_next | syscall\_exit\_to\_user\_mode |
| Attack | 174 | 192 | 161 | 156 | 144 |
| Normal | 195 | 155 | 176 | 164 | 162 |
| Exclusive | Feature Name | tcp\_recvmsg\_locked | tcp\_sendmsg\_locked | skb\_page\_frag\_refill | pick\_next\_task\_fair | perf\_event\_update\_time |
| Attack | 103 | 87 | 49 | 39 | 27 |
| Normal | 103 | 87 | 49 | 39 | 27 |
| All | Feature Name | psi\_group\_change | perf\_event\_update\_userpage | merge\_sched\_in | rb\_next | syscall\_exit\_to\_user\_mode |
| Attack | 174 | 192 | 161 | 156 | 144 |
| Normal | 195 | 155 | 176 | 164 | 162 |
| Instructions | Common | Feature Name | psi\_group\_change | merge\_sched\_in | event\_sched\_in | native\_sched\_clock | rb\_next |
| Attack | 196 | 189 | 186 | 143 | 116 |
| Normal | 204 | 200 | 199 | 119 | 110 |
| Exclusive | Feature Name | tcp\_write\_xmit | tcp\_clean\_rtx\_queue.constprop.0 | \_\_virt\_addr\_valid | dequeue\_task | ip\_finish\_output2 |
| Attack | 89 | 56 | 35 | 38 | 34 |
| Normal | 89 | 56 | 35 | 38 | 34 |
| All | Feature Name | psi\_group\_change | merge\_sched\_in | event\_sched\_in | native\_sched\_clock | rb\_next |
| Attack | 196 | 189 | 186 | 143 | 116 |
| Normal | 204 | 200 | 199 | 119 | 110 |
| wid\_rcon\_go | Branch | Common | Feature Name | merge\_sched\_in | psi\_group\_change | visit\_groups\_merge.constprop.0.is | event\_sched\_in | iterate\_groups |
| Attack | 9 | 8 | 8 | 5 | 8 |
| Normal | 33 | 33 | 32 | 30 | 24 |
| Exclusive | Feature Name | prepare\_task\_switch | netif\_skb\_features | perf\_event\_update\_time | reweight\_entity | \_\_sk\_dst\_check |
| Attack | 24 | 22 | 21 | 17 | 17 |
| Normal | 24 | 22 | 21 | 17 | 17 |
| All | Feature Name | merge\_sched\_in | psi\_group\_change | prepare\_task\_switch | visit\_groups\_merge.constprop.0.is | netif\_skb\_features |
| Attack | 9 | 8 | 24 | 8 | 22 |
| Normal | 33 | 33 | 24 | 32 | 22 |
| Cycles | Common | Feature Name | perf\_event\_update\_userpage | syscall\_exit\_to\_user\_mode | psi\_group\_change | merge\_sched\_in | syscall\_return\_via\_sysret |
| Attack | 13 | 10 | 11 | 13 | 7 |
| Normal | 36 | 38 | 36 | 21 | 28 |
| Exclusive | Feature Name | arch\_perf\_update\_userpage | tcp\_recvmsg\_locked | iterate\_groups | sk\_stream\_alloc\_skb | tcp\_rcv\_established |
| Attack | 20 | 20 | 10 | 18 | 17 |
| Normal | 20 | 20 | 10 | 18 | 17 |
| All | Feature Name | perf\_event\_update\_userpage | syscall\_exit\_to\_user\_mode | psi\_group\_change | merge\_sched\_in | syscall\_return\_via\_sysret |
| Attack | 13 | 10 | 11 | 13 | 7 |
| Normal | 36 | 38 | 36 | 21 | 28 |
| Instructions | Common | Feature Name | merge\_sched\_in | event\_sched\_in | psi\_group\_change | perf\_event\_groups\_first | native\_sched\_clock |
| Attack | 13 | 12 | 12 | 9 | 11 |
| Normal | 32 | 30 | 30 | 26 | 18 |
| Exclusive | Feature Name | arch\_perf\_update\_userpage | \_\_sk\_dst\_check | ip\_rcv\_core | \_\_inet\_lookup\_established | \_\_alloc\_skb |
| Attack | 26 | 13 | 19 | 18 | 17 |
| Normal | 26 | 13 | 19 | 18 | 17 |
| All | Feature Name | merge\_sched\_in | event\_sched\_in | psi\_group\_change | arch\_perf\_update\_userpage | \_\_sk\_dst\_check |
| Attack | 13 | 12 | 12 | 26 | 13 |
| Normal | 32 | 30 | 30 | 26 | 13 |

Tables 31 and 32 show the final feature sizes of the CS and GS generated in this study. The number of basic features used in this study is 5, so only the sizes of these basic features are listed under each attack scenario. These features are used to generate 31 feature combinations in the "Common," "Exclusive," and "All" fields, respectively, in those tables. Table 31 has a "N/A" field, but Table 32 does not. Since there are three CS, a symbol as a feature candidate must exist in all CS. If not, it is considered "N/A." However, since only one GS exists, "N/A" does not apply to Table 32.

Table 33. symbol list for the pseudo-code for CSR

|  |  |  |  |
| --- | --- | --- | --- |
| Symbol | Explanation | Symbol | Explanation |
| len() | a function that calculates the size of a feature | asr | averaged sampling resolution |
| n | symbol count | temp | Temporal variable |
| sl | symbol list | asrd | averaged sampling resolution difference |
| st | simulation time on an attack scenario | exp | exponential |
| sr | sampling resolution | csr | combined sampling resolution |
| m | cs count | sc | sampling count |

텍스트, 친필, 폰트, 문서이(가) 표시된 사진

자동 생성된 설명

Figure 24. Pseudo-code for CSR

Table 33 and Figure 24 show the pseudo code proposed to calculate the CSR in this study. Since the CSR represents the loss of feature information, the degree of loss can be estimated by comparing the information of the original feature with the CSR value.

### Proof

Let means a CSR value of a feature combination refers to a list of the overheads of a symbol on a CS. def. and . As we use three CS in this paper, the range of the CS is set to , . In Table 29, we compare the information loss rate and CSR of feature combinations consisting of 5 basic symbols of CS. We refer to the "common" type of CSR and information loss rate. The reason is that symbols exist in attack and normal modes. def. , , . s.t. is a histogram built with overhead data extracted from the original TOP dataset without the feature downsizing method. is a histogram of overheads extracted from the TOP dataset to which the downsized technique has been applied. s.t. The Information Loss Rate (ILR) is calculated as follows.

* ,

The represents the difference between histogram values on the overheads of an original symbol and the other overheads after applying feature downsizing. The histograms have 100 ranks from 0 to 99, and the interval is one as is 100. The represents the average IL R for each . The represents the final ILR for a feature combination of 5 basic symbols as is 1~5.

Table 34. Comparison of CSR and ILR of the Basic Features

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Index | Scenario | Category | Basic Feature Name | Attack Mode | | Normal Mode | |
| CSR |  | CSR |  |
| 1 | cid\_rcoff\_goff | Branch | psi\_group\_change | 0.432 | 0.241 | 0.189 | 0.241 |
| perf\_event\_groups\_insert | 0.278 | 0.142 | 0.1 | 0.142 |
| event\_sched\_in | 0.187 | 0.103 | 0.174 | 0.103 |
| merge\_sched\_in | 0.226 | 0.11 | 0.116 | 0.11 |
| kmem\_cache\_alloc\_trace | 0.181 | 0.097 | 0.076 | 0.097 |
| Cycle | perf\_event\_alloc | 0.385 | 0.17 | 0.076 | 0.17 |
| Instruction | psi\_group\_change | 0.346 | 0.183 | 0.143 | 0.183 |
| event\_sched\_in | 0.195 | 0.122 | 0.103 | 0.122 |
| inherit\_event.constprop.0 | 0.194 | 0.094 | 0.118 | 0.094 |
| native\_sched\_clock | 0.157 | 0.068 | 0.086 | 0.068 |
| x86\_pmu\_event\_init | 0.11 | 0.094 | 0.077 | 0.094 |
| 2 | cid\_rcon\_goff | Branch | psi\_group\_change | 0.341 | 0.161 | 0.2 | 0.161 |
| event\_sched\_in | 0.131 | 0.074 | 0.192 | 0.074 |
| merge\_sched\_in | 0.205 | 0.094 | 0.149 | 0.094 |
| kmem\_cache\_alloc\_node\_trace | 0.169 | 0.084 | 0.1 | 0.084 |
| kmem\_cache\_alloc\_trace | 0.142 | 0.069 | 0.094 | 0.069 |
| Cycle | memset\_erms | 0.339 | 0.171 | 0.262 | 0.171 |
| psi\_group\_change | 0.216 | 0.111 | 0.269 | 0.111 |
| syscall\_exit\_to\_user\_mode | 0.181 | 0.082 | 0.247 | 0.082 |
| perf\_event\_update\_userpage | 0.172 | 0.08 | 0.263 | 0.08 |
| entry\_SYSCALL\_64\_after\_hwframe | 0.142 | 0.064 | 0.263 | 0.064 |
| Instruction | psi\_group\_change | 0.273 | 0.123 | 0.217 | 0.123 |
| perf\_event\_alloc | 0.242 | 0.1 | 0.207 | 0.1 |
| kfree | 0.335 | 0.149 | 0.103 | 0.149 |
| kmem\_cache\_alloc\_node | 0.242 | 0.094 | 0.09 | 0.094 |
| merge\_sched\_in | 0.22 | 0.092 | 0.121 | 0.092 |
| 3 | cid\_rcon\_gon | Branch | psi\_group\_change | 0 | 0 | 0.234 | 0 |
| inherit\_event.constprop.0 | 0 | 0 | 0.208 | 0 |
| native\_sched\_clock | 0 | 0 | 0.189 | 0 |
| perf\_event\_alloc | 0 | 0 | 0.098 | 0 |
| memset\_erms | 0 | 0 | 0.081 | 0 |
| Cycle | psi\_group\_change | 0 | 0 | 0.274 | 0 |
| memset\_erms | 0 | 0 | 0.262 | 0 |
| inherit\_task\_group.isra.0 | 0 | 0 | 0.186 | 0 |
| perf\_event\_alloc | 0 | 0 | 0.175 | 0 |
| rb\_next | 0 | 0 | 0.166 | 0 |
| Instruction | psi\_group\_change | 0 | 0 | 0.213 | 0 |
| perf\_event\_alloc | 0 | 0 | 0.196 | 0 |
| event\_sched\_in | 0 | 0 | 0.196 | 0 |
| kfree | 0 | 0 | 0.15 | 0 |
| perf\_event\_groups\_first | 0 | 0 | 0.101 | 0 |
| 4 | wct\_rcoff\_gon | Branch | psi\_group\_change | 0.134 | 0.028 | 0.266 | 0.028 |
| x86\_pmu\_enable | 0.017 | 0.006 | 0.009 | 0.006 |
| Cycle | perf\_event\_update\_userpage | 0.093 | 0.022 | 0.329 | 0.022 |
| memset\_erms | 0.11 | 0.014 | 0.275 | 0.014 |
| syscall\_exit\_to\_user\_mode | 0.089 | 0.018 | 0.137 | 0.018 |
| entry\_SYSCALL\_64\_after\_hwframe | 0.09 | 0.014 | 0.162 | 0.014 |
| perf\_event\_alloc | 0.079 | 0.02 | 0.138 | 0.02 |
| Instruction | perf\_event\_alloc | 0.142 | 0.031 | 0.101 | 0.031 |
| \_\_intel\_pmu\_enable\_all.constprop. | 0.017 | 0.002 | 0.009 | 0.002 |
| 5 | wct\_rcon\_goff | Branch | psi\_group\_change | 0.389 | 0.164 | 0.205 | 0.164 |
| kmem\_cache\_alloc\_node | 0.232 | 0.09 | 0.196 | 0.09 |
| perf\_event\_groups\_insert | 0.21 | 0.128 | 0.185 | 0.128 |
| event\_sched\_in | 0.231 | 0.105 | 0.161 | 0.105 |
| merge\_sched\_in | 0.081 | 0.077 | 0.15 | 0.077 |
| Cycle | memset\_erms | 0.395 | 0.157 | 0.144 | 0.157 |
| perf\_event\_alloc | 0.386 | 0.136 | 0.133 | 0.136 |
| inherit\_event.constprop.0 | 0.244 | 0.107 | 0.22 | 0.107 |
| psi\_group\_change | 0.128 | 0.052 | 0.242 | 0.052 |
| syscall\_exit\_to\_user\_mode | 0.18 | 0.092 | 0.134 | 0.092 |
| Instruction | psi\_group\_change | 0.315 | 0.117 | 0.321 | 0.117 |
| kfree | 0.379 | 0.141 | 0.158 | 0.141 |
| perf\_event\_alloc | 0.226 | 0.146 | 0.162 | 0.146 |
| rb\_next | 0.199 | 0.121 | 0.129 | 0.121 |
| merge\_sched\_in | 0.161 | 0.058 | 0.222 | 0.058 |
| 6 | wct\_rcon\_gon | Branch | psi\_group\_change | 0.106 | 0.015 | 0.32 | 0.015 |
| x86\_get\_event\_constraints | 0.08 | 0.014 | 0.101 | 0.014 |
| x86\_pmu\_enable | 0.018 | 0.002 | 0.018 | 0.002 |
| Cycle | memset\_erms | 0.097 | 0.019 | 0.142 | 0.019 |
| native\_write\_msr | 0.06 | 0.004 | 0.085 | 0.004 |
| Instruction | psi\_group\_change | 0.088 | 0.022 | 0.273 | 0.022 |
| perf\_event\_alloc | 0.063 | 0.011 | 0.197 | 0.011 |
| 7 | wet\_rcoff\_goff | Branch | psi\_group\_change | 0.421 | 0.252 | 0.202 | 0.252 |
| perf\_event\_groups\_insert | 0.351 | 0.175 | 0.091 | 0.175 |
| rb\_next | 0.26 | 0.117 | 0.099 | 0.117 |
| merge\_sched\_in | 0.172 | 0.112 | 0.141 | 0.112 |
| memset\_erms | 0.199 | 0.146 | 0.133 | 0.146 |
| Cycle | memset\_erms | 0.379 | 0.205 | 0.079 | 0.205 |
| perf\_event\_alloc | 0.285 | 0.169 | 0.078 | 0.169 |
| syscall\_exit\_to\_user\_mode | 0.219 | 0.163 | 0.146 | 0.163 |
| psi\_group\_change | 0.146 | 0.107 | 0.126 | 0.107 |
| event\_sched\_in | 0.103 | 0.092 | 0.169 | 0.092 |
| Instruction | psi\_group\_change | 0.396 | 0.195 | 0.207 | 0.195 |
| perf\_event\_alloc | 0.263 | 0.152 | 0.172 | 0.152 |
| kfree | 0.298 | 0.175 | 0.121 | 0.175 |
| event\_sched\_in | 0.247 | 0.099 | 0.104 | 0.099 |
| visit\_groups\_merge.constprop.0.is | 0.128 | 0.047 | 0.191 | 0.047 |
| 8 | wet\_rcon\_goff | Branch | psi\_group\_change | 0.368 | 0.158 | 0.296 | 0.158 |
| event\_sched\_in | 0.215 | 0.073 | 0.205 | 0.073 |
| kmem\_cache\_alloc\_node\_trace | 0.185 | 0.075 | 0.217 | 0.075 |
| perf\_event\_update\_userpage | 0.174 | 0.07 | 0.195 | 0.07 |
| perf\_event\_\_id\_header\_size | 0.164 | 0.064 | 0.193 | 0.064 |
| Cycle | memset\_erms | 0.422 | 0.14 | 0.222 | 0.14 |
| psi\_group\_change | 0.271 | 0.074 | 0.305 | 0.074 |
| rb\_next | 0.268 | 0.049 | 0.231 | 0.049 |
| kmem\_cache\_alloc\_node | 0.236 | 0.082 | 0.215 | 0.082 |
| syscall\_return\_via\_sysret | 0.236 | 0.063 | 0.207 | 0.063 |
| Instruction | psi\_group\_change | 0.392 | 0.227 | 0.313 | 0.227 |
| native\_sched\_clock | 0.258 | 0.101 | 0.207 | 0.101 |
| kmem\_cache\_alloc\_trace | 0.161 | 0.097 | 0.207 | 0.097 |
| \_\_srcu\_read\_lock | 0.15 | 0.095 | 0.207 | 0.095 |
| perf\_event\_groups\_insert | 0.115 | 0.08 | 0.238 | 0.08 |
| 9 | wid\_rcon\_goff | Branch | psi\_group\_change | 0.364 | 0.19 | 0.229 | 0.19 |
| perf\_event\_alloc | 0.264 | 0.264 | 0.185 | 0.091 |
| merge\_sched\_in | 0.252 | 0.125 | 0.123 | 0.125 |
| inherit\_event.constprop.0 | 0.269 | 0.14 | 0.119 | 0.14 |
| event\_sched\_in | 0.17 | 0.067 | 0.116 | 0.067 |
| Cycle | memset\_erms | 0.403 | 0.152 | 0.082 | 0.152 |
| perf\_event\_alloc | 0.363 | 0.135 | 0.095 | 0.135 |
| psi\_group\_change | 0.181 | 0.093 | 0.229 | 0.093 |
| merge\_sched\_in | 0.158 | 0.071 | 0.218 | 0.071 |
| syscall\_return\_via\_sysret | 0.215 | 0.09 | 0.117 | 0.09 |
| Instruction | psi\_group\_change | 0.41 | 0.145 | 0.308 | 0.145 |
| perf\_event\_alloc | 0.395 | 0.154 | 0.183 | 0.154 |
| perf\_event\_groups\_insert | 0.215 | 0.116 | 0.218 | 0.116 |
| kfree | 0.238 | 0.109 | 0.126 | 0.109 |
| merge\_sched\_in | 0.131 | 0.109 | 0.148 | 0.076 |
| 10 | wid\_rcon\_go | Branch | x86\_pmu\_enable | 0.018 | 0.004 | 0.041 | 0.004 |
| Cycle | syscall\_exit\_to\_user\_mode | 0.05 | 0.006 | 0.149 | 0.006 |
| native\_write\_msr | 0.018 | 0.006 | 0.009 | 0.006 |
| Instruction | kfree | 0.064 | 0.013 | 0.189 | 0.013 |

Table 34 lists CSR and ILR for basic symbols in the ten attack scenarios. Some scenarios with zero values of the ILR and CSR are excluded from this table because they are invalid for this proof in both attack and normal modes. CSR and ILR are indicators that quantitatively represent the magnitude of information loss. In this regard, the indicators will show similar distributions based on an identical feature combination of an attack scenario.

Figure 25. Analysis of information loss on the feature combination of the basic features, cf.

Figure 26. Analysis of information loss on the feature combination of the basic features, cf.

Figures 25 and 26 show the comparisons of the CSR values with the downsizing method and the values ​​of the original feature without the method. The CSR and are calculated on the feature combinations of the basic symbols in Table 34. Although the CSR values are greater than the values, the two values ​​increase or decrease in a similar pattern. Therefore, if we compare the two patterns and confirm a correlation, we can determine that CSR and correlate to each other. The major models of correlation analysis are classified into Pearson's or Spearman's correlation analysis. Pearson’s model [49] has a drawback in that the coefficient accuracy is low if the data points of the population do not follow a normal distribution. On the other hand, Spearman's model [50] does not care if the data points are not normally distributed. However, Spearman's model is used to verify the correlation of the order of the data. Since the data in Figures 25 and 26 do not follow a normal distribution and each bar represents an order of the value size, it is appropriate to apply Spearman's correlation analysis in this proof.

텍스트, 스크린샷, 폰트, 번호이(가) 표시된 사진

자동 생성된 설명

Figure 27. Spearman’s correlation analysis on the CSR and in Figures 25 and 26

Figure 27 shows the result of Spearman's correlation analysis based on the CSR and results of Figures 25 and 26. “statistic" means a correlation coefficient [51], indicating a strong positive correlation if the coefficient value is more than 0.6. "p\_value" [52] is a probability value obtained through a non-parametric test. Generally, the null hypothesis is adopted when the value is greater than 0.05, and the alternative hypothesis is accepted when it is less than or equal to 0.05.

According to "decision," the result of Figure 27 shows that "statistic" values ​​are greater than or equal to 0.6 and "p\_value" values ​​are less than or equal to 0.05. Therefore, we reject the null hypothesis and accept the alternative hypothesis. CSR and have a strong correlation and satisfy the significance level of 5%.

Experiment Result

This section presents experimental results on the methodologies mentioned in the previous section. For the best feature combination of Perf STAT and Time Delta, we should choose the best one with low CLR to minimize information loss. On the other hand, for the best combination of Perf TOP, we have to choose the best one with high CSR. Perf STAT and Time Delta features are based on CLR because the number of data points does not go to zero in the attack and normal modes. However, Perf TOP features are based on CSR because some features exist only in either attack or normal mode.

### Various ML Implementations for DDoS Detection

Table 35. Machine learning algorithms used in this paper (N/A: Not Available)

|  |  |  |
| --- | --- | --- |
| ML Type | ML Name | Parameters |
| Supervised Learning | ADA Boost (AB) | random\_state = 0 |
| Decision Tree (DT) | random\_state = 0 |
| Gaussian Naïve Bayes (GNB) | N/A |
| Gradient Boost (GB) | max\_depth = 2, learning\_rate = 0.01, random\_state = 0 |
| K Nearest Neighbor (KNN) | n\_neighbors = 2 |
| Linear Regression (LR) | N/A |
| Ridge Regression (RR) | alpha = 1 |
| Lasso Regression (LaR) | alpha = 0.01 |
| Elasatic Net (EN) | alpha = 0.01, l1\_ratio = 0.01 |
| Logistic Regression (LoR) | penalty = 'l2' |
| Random Forest (RF) | max\_depth = 2, random\_state = 0 |
| Support Vector Machine (SVM) | kernel = 'linear', random\_state = 0 |
| Unsupervised Learning | Agglomerative Clustering (AC) | n\_clusters = 2, linkage = 'complete' |
| DB Scan (DS) | eps=250000000 |
| Gaussian Mixture (GM) | n\_components = 2, random\_state = 0, reg\_covar = 10 |
| K Means (KM) | n\_clusters = 2, init = 'random', n\_init = 'auto', max\_iter = 100, random\_state = 0 |
| Deep Learning | Deep Neural Network (DNN) | Dense(units = 20) BatchNormalization(), Activation('relu'), Dense(units = 2), Activation(‘softmax’) |

Table 35 lists the ML algorithms used in this study. These algorithms were referenced from Python Keras version 2.12.0 [53] and Scikit-Learn version 1.2.2 [54] libraries. Parameters not specified in the table were applied with the default values ​​of the libraries. The ML dataset we used is CICEV2023, published in this paper [1] and discussed in the methodology section.

## Feature Selection

Table 36. Best ML Result of the Perf STAT and Time Delta on CS and GS (SM: Support Mean, FC: Feature Combination, B: Branch, C: Cycle, I: Instruction)

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Scenario | Station Type | FC | ML Type | CLR | F1 Score | Support | CLR Mean | F1 Mean | SM |
| cid\_rcoff\_goff | CS | B + C + I | AB | 0.118 | 0.993 | 2187 | 1.854 | 0.971 | 1408 |
| GS | B + C + I | KNN | 0 | 0.983 | 1861 | 0.825 | 0.958 | 1256 |
| cid\_rcoff\_gon | CS | B + I | AB | 0.458 | 0.79 | 207 | 1.324 | 0.776 | 167 |
| GS | B + C + I | GB | 0 | 0.944 | 865 | 6.964 | 0.857 | 4744 |
| cid\_rcon\_goff | CS | B + C + I | AB | 0.061 | 0.96 | 1225 | 1.243 | 0.943 | 936 |
| GS | B + C + I | AB | 0 | 0.973 | 1058 | 0.678 | 0.945 | 859 |
| cid\_rcon\_gon | CS | B + C + I | AB | 0.471 | 0.865 | 207 | 1.194 | 0.812 | 174 |
| GS | B + C + I | AB | 0 | 0.842 | 196 | 0.735 | 0.768 | 168 |
| wct\_rcoff\_goff | CS | B + C | AB | 0.111 | 0.994 | 2188 | 1.852 | 0.974 | 1409 |
| GS | C + I | AB | 0 | 0.986 | 1862 | 0.826 | 0.958 | 1257 |
| wct\_rcoff\_gon | CS | B + C + I | AB | 0.548 | 0.856 | 196 | 1.129 | 0.804 | 162 |
| GS | B + C | RF | 0 | 0.783 | 196 | 0.761 | 0.783 | 162 |
| wct\_rcon\_goff | CS | B | GB | 0.062 | 0.973 | 1190 | 1.265 | 0.952 | 912 |
| GS | B + C + I | AB | 0 | 0.957 | 1028 | 0.726 | 0.94 | 836 |
| wct\_rcon\_gon | CS | B + C + I | AB | 0.569 | 0.843 | 192 | 1.241 | 0.8 | 160 |
| GS | B + C | RF | 0 | 0.803 | 194 | 0.729 | 0.796 | 161 |
| wet\_rcoff\_goff | CS | B + C + I | AB | 0.108 | 0.969 | 2076 | 1.798 | 0.952 | 1357 |
| GS | B + C + I | KNN | 0 | 0.965 | 1302 | 0.59 | 0.951 | 965 |
| wet\_rcoff\_gon | CS | B + I | RF | 0.524 | 0.888 | 200 | 1.325 | 0.825 | 164 |
| GS | B + C + I | AB | 0 | 0.822 | 198 | 0.777 | 0.784 | 163 |
| wet\_rcon\_goff | CS | B | RF | 0 | 0.914 | 1094 | 1.274 | 0.894 | 845 |
| GS | C + I | RF | 0 | 0.942 | 749 | 1.345 | 0.921 | 582 |
| wet\_rcon\_gon | CS | B + C + I | AB | 0.64 | 0.842 | 195 | 1.465 | 0.793 | 159 |
| GS | I | KM | 0 | 0.56 | 136 | 0.578 | 0.654 | 131 |
| wid\_rcoff\_goff | CS | B + I | AB | 0.109 | 0.997 | 2187 | 1.848 | 0.982 | 1408 |
| GS | B + C + I | AB | 0 | 0.981 | 1887 | 0.842 | 0.957 | 1268 |
| wid\_rcoff\_gon | CS | B + I | AB | 0.528 | 0.808 | 203 | 1.308 | 0.802 | 165 |
| GS | B + C + I | RF | 0 | 0.793 | 209 | 0.809 | 0.796 | 168 |
| wid\_rcon\_goff | CS | B + C | AB | 0.083 | 0.939 | 1296 | 1.284 | 0.924 | 985 |
| GS | C + I | AB | 0 | 0.95 | 1102 | 0.678 | 0.933 | 895 |
| wid\_rcon\_gon | CS | B + I | AB | 0.499 | 0.807 | 194 | 1.231 | 0.803 | 161 |
| GS | B + C + I | DT | 0 | 0.83 | 200 | 0.796 | 0.796 | 164 |

Table 36 shows the results of ML implementations on the various feature combinations of the Perf STAT and Time Delta for the different scenarios in CS and GS. "ML Type" is referenced in the "ML Name" field of Table 35. "Support" means the data point size of a feature combination. In each of the scenarios in Table 2, ML classification was performed on the feature combinations in Table 6. We sorted these ML results in order of high support value, low CLR value, and high F1 score. A feature combination that satisfies the three sorting criteria is recommended as the best feature combination in each scenario. "CLR Mean" is the average CLR value calculated for all feature combinations in a scenario. "F1 Mean" represents the average of the F1 values ​​for all feature combinations in a scenario. "SM" means the average of the feature sizes of all feature combinations in a scenario.

Figure 27. Proof of the low CLR of the best feature combination in each scenario in Table 36

Figure 28. Proof of the high F1 score of the best feature combination in each scenario in Table 36

Figure 29. Proof of the high Support of the best feature combination in each scenario in Table 36

Figures 27, 28, and 29 are the bar graphs of the CLR, F1, and Support values ​​and their average values ​​from Table 36. The criterion for selecting the optimal feature combination proves appropriate since the CLR values ​​are below average, and the F1 and support values ​​are above average.

### Suggestion on the Best Feature Combination and ML

Table 37. Best ML Result of the Perf TOP on CS and GS

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Scenario | Station Type | Type 1 | Type 2 | Feature Combination | ML Type | CSR | F1 | Support | F1 Mean | Support Mean | CSR Mean |
| cid\_rcoff\_goff | CS | instruction | exclusive | kfree | AB | 0.178 | 1.0 | 162 | 0.825 | 65 | 0.183 |
| GS | branch | all | psi\_group\_change | DT | 0.458 | 0.787 | 2177 | 0.757 | 111 | 0.321 |
| cid\_rcoff\_gon | CS | branch | exclusive | psi\_group\_change, event\_sched\_in | AB | 0.162 | 1.0 | 14 | 0.767 | 4 | 0.071 |
| GS | branch | common | psi\_group\_change | AB | 3.264 | 0.893 | 120 | 0.805 | 69 | 1.439 |
| cid\_rcon\_goff | CS | cycles | all | memset\_erms | DT | 0.301 | 0.859 | 78 | 0.805 | 38 | 0.204 |
| GS | instructions | common | psi\_group\_change | DT | 0.44 | 0.658 | 118 | 0.72 | 60 | 0.315 |
| cid\_rcon\_gon | CS | cycles | exclusive | psi\_group\_change,  syscall\_exit\_to\_user\_mode,  memset\_erms | AB | 0.199 | 1.0 | 16 | 0.866 | 8 | 0.136 |
| GS | instructions | exclusive | rb\_next, event\_sched\_in | AB | 0.226 | 1.0 | 22 | 0.822 | 11 | 0.219 |
| wct\_rcoff\_goff | CS | branch | exclusive | psi\_group\_change | AB | 0.206 | 1.0 | 190 | 0.855 | 74 | 0.15 |
| GS | instructions | common | psi\_group\_change | AB | 0.455 | 0.724 | 255 | 0.767 | 118 | 0.327 |
| wct\_rcoff\_gon | CS | branch | exclusive | event\_sched\_in | AB | 0.104 | 1.0 | 12 | 0.582 | 2.319 | 0.015 |
| GS | instructions | exclusive | sched\_clock\_cpu | AB | 0.168 | 1.0 | 22 | 0.825 | 10 | 0.209 |
| wct\_rcon\_goff | CS | instructions | all | psi\_group\_change | AB | 0.318 | 0.875 | 80 | 0.809 | 34 | 0.211 |
| GS | instructions | all | psi\_group\_change | GN | 0.432 | 0.64 | 112 | 0.727 | 67 | 0.347 |
| wct\_rcon\_gon | CS | branch | exclusive | rb\_next | AB | 0.128 | 1.0 | 14 | 0.352 | 2 | -0.184 |
| GS | cycles | exclusive | merge\_sched\_in | AB | 0.158 | 1.0 | 20 | 0.814 | 11 | 0.231 |
| wet\_rcoff\_goff | CS | branch | common | psi\_group\_change | DT | 0.311 | 0.978 | 137 | 0.8 | 49 | 0.187 |
| GS | branch | common | psi\_group\_change | DT | 0.444 | 0.809 | 199 | 0.702 | 101 | 0.312 |
| wet\_rcoff\_gon | CS | branch | exclusive | psi\_group\_change, merge\_sched\_in | AB | 0.178 | 1.0 | 16 | 0.848 | 5 | 0.117 |
| GS | cycles | exclusive | event\_sched\_in | AB | 0.159 | 1.0 | 20 | 0.814 | 10 | 0.226 |
| wet\_rcon\_goff | CS | instructions | common | psi\_group\_change | RF | 0.352 | 0.864 | 83 | 0.787 | 48 | 0.228 |
| GS | instructions | common | psi\_group\_change | GB | 0.438 | 0.691 | 104 | 0.703 | 56 | 0.321 |
| wet\_rcon\_gon | CS | instructions | exclusive | psi\_group\_change | AB | 0.143 | 1.0 | 16 | 0.819 | 3 | 0.097 |
| GS | branch | common | \_\_perf\_event\_task\_sched\_in,  psi\_group\_change | AC | 0.227 | 0.619 | 8 | 0.261 | 5 | 0.175 |
| wid\_rcoff\_goff | CS | branch | exclusive | psi\_group\_change | AB | 0.195 | 1.0 | 176 | 0.85 | 63 | 0.153 |
| GS | branch | all | psi\_group\_change | GB | 0.454 | 0.754 | 214 | 0.748 | 116 | 0.333 |
| wid\_rcoff\_gon | CS | cycles | exclusive | perf\_event\_alloc | AB | 0.131 | 1.0 | 14 | 0.778 | 5 | 0.134 |
| GS | instructions | exclusive | skb\_release\_data | AB | 0.167 | 1.0 | 22 | 0.836 | 10 | 0.194 |
| wid\_rcon\_goff | CS | instructions | all | psi\_group\_change | KNN | 0.359 | 0.854 | 96 | 0.792 | 4 | 0.103 |
| GS | branch | all | psi\_group\_change | RF | 0.436 | 0.666 | 122 | 0.714 | 66 | 0.324 |
| wid\_rcon\_gon | CS | instructions | exclusive | psi\_group\_change | AB | 0.168 | 1.0 | 20 | 0.795 | 34 | 0.211 |
| GS | instructions | exclusive | arch\_perf\_update\_userpage | AB | 0.124 | 1.0 | 16 | 0.808 | 9 | 0.228 |

Table 37 shows the results of performing various attack detection MLs on different feature combinations of the Perf TOP in CS and GS. We performed the MLs on the feature combinations of "Symbol Set" for "Type 1" and "Type 2" in Tables 29 and 30. We selected the best feature combinations in each scenario based on high values ​​in the order of CSR, F1, and Support.

Figure 30. Proof of the high CSR of the best feature combination in each scenario in Table 36

Figure 31. Proof of the high F1 score of the best feature combination in each scenario in Table 36

Figure 32. Proof of the high Support of the best feature combination in each scenario in Table 36

Figures 30, 31, and 32 refer to the "CSR," "F1", "Support," "F1 Mean", "Support Mean," and "CSR Mean" fields of Table 37. The figures show that most CSR, F1 score, and Support values ​​are generally higher than their averages. Thus, the criterion with the high values is valid for extracting the best feature combination of the Perf TOP.

Figure 33. Means of F1 scores from Time Deltas under different attack scenarios

Figure 33 shows the average of the F1 scores for the Time Delta feature under various attack scenarios in CS and GS. The scores under half of the attack scenarios show values ​​of about 0.5 and 0.7 under the other attack scenarios. These F1 scores indicate that the attack detection model is inaccurate when using only the Time Delta feature except for the Perf TOP and Perf STAT.

Figure 34. Means of Support from Time Deltas under different attack scenarios

Figure 34 shows the average number of data points for Time Delta features in Figure 33. The number of data points for the Time Delta feature is generally similar to or higher than the size of the Perf TOP feature.

Conclusion

This study proposes the best feature combination for DDoS attack detection ML in EV charging infrastructure. Features are extracted under Sixteen attack scenarios, and ML classification for attack and normal is performed. These scenarios based on DDoS attacks cause many intentional authentication failures, preventing other legitimate EVs from charging. Feature types consist of Perf STAT: consumed cycle, consumed instruction, and consumed branch and Perf TOP: kernel overheads on the EV-CS-GS virtual infrastructure. In addition, we use Time Delta as a general DDoS-related feature representing the difference between EV authentication time intervals. This feature enables us to compare our new features with the existing ones in general network environments regarding ML classification accuracy. If the sizes of the features differ in combining them, they are downsized to the smallest feature size.

This feature downsizing technique is a novel downsampling method proposed in this paper. Feature upsampling was not applied because we found a divergence problem when reconstructing small features to large feature sizes. The feature downsizing method is designed to minimize feature information loss. After performing various ML algorithms on different feature combinations, feature combinations are recommended based on low information loss rate, high combined sampling resolution, high F1 score, and large feature size. Detailed information about the features has been described in the tables. The minimization of information loss in our proposed feature downsizing technique was demonstrated through multiple regression analysis. In addition, the validity of the high combined sampling resolution was verified by Spearman's correlation analysis. Based on the feature combinations of Perf TOP, Perf STAT, and Time Delta, 17 different ML algorithms were performed to get the best feature combination for each scenario. We confirmed that the classification accuracy was higher when Perf TOP and Perf STAT were used together than when only the Time Delta feature was used.

References

1. PST Conference
2. Kaveh, M., Martín, D., & Mosavi, M. R. (2020). A lightweight authentication scheme for V2G communications: A PUF-based approach ensuring cyber/physical security and identity/location privacy. *Electronics*, *9*(9), 1479.
3. Bansal, G., Naren, N., & Chamola, V. (2020, January). Rama: Real-time automobile mutual authentication protocol using puf. In *2020 International Conference on Information Networking (ICOIN)* (pp. 265-270). IEEE.
4. Sharma, G., Joshi, A. M., & Mohanty, S. P. (2021, December). An efficient physically unclonable function based authentication scheme for V2G network. In *2021 IEEE International Symposium on Smart Electronic Systems (iSES)(Formerly iNiS)* (pp. 421-425). IEEE.
5. Babu, P. R., Palaniswamy, B., Reddy, A. G., Odelu, V., & Kim, H. S. (2022). A survey on security challenges and protocols of electric vehicle dynamic charging system. *Security and Privacy*, *5*(3), e210.

Parameswarath, R. P., Gope, P., & Sikdar, B. (2022). User-empowered privacy-preserving authentication protocol for electric vehicle charging based on decentralized identity and verifiable credential. *ACM Transactions on Management Information Systems (TMIS)*, *13*(4), 1-21.

1. ElGhanam, E., Ahmed, I., Hassan, M., & Osman, A. (2021). Authentication and billing for dynamic wireless EV charging in an internet of electric vehicles. *Future Internet*, *13*(10), 257.
2. Almuhaideb, A. M., & Algothami, S. S. (2022). ECQV-Based Lightweight Revocable Authentication Protocol for Electric Vehicle Charging. *Big Data and Cognitive Computing*, *6*(4), 102.
3. Babu, P. R., Reddy, A. G., Palaniswamy, B., & Kommuri, S. K. (2022). EV-Auth: Lightweight authentication protocol suite for dynamic charging system of electric vehicles with seamless handover. *IEEE Transactions on Intelligent Vehicles*, *7*(3), 734-747.
4. Chen, C. M., Hao, Y., & Wu, T. Y. (2023). Discussion of "Ultra Super Fast Authentication Protocol for Electric Vehicle Charging Using Extended Chaotic Maps". *IEEE Transactions on Industry Applications*, *59*(2), 2091-2092.
5. Bansal, G., Naren, N., Chamola, V., Sikdar, B., Kumar, N., & Guizani, M. (2020). Lightweight mutual authentication protocol for V2G using physical unclonable function. *IEEE Transactions on Vehicular Technology*, *69*(7), 7234-7246.
6. Babu, P. R., Amin, R., Reddy, A. G., Das, A. K., Susilo, W., & Park, Y. (2021). Robust authentication protocol for dynamic charging system of electric vehicles. *IEEE Transactions on Vehicular Technology*, *70*(11), 11338-11351.
7. Lee, Z., Johansson, D., & Low, S. H. (2019, June). ACN-sim: An open-source simulator for data-driven electric vehicle charging research. In *Proceedings of the Tenth ACM International Conference on Future Energy Systems* (pp. 411-412).
8. Weaver, V. M. (2015, March). Self-monitoring overhead of the Linux perf\_ event performance counter interface. In *2015 IEEE International Symposium on Performance Analysis of Systems and Software (ISPASS)* (pp. 102-111). IEEE.
9. Irelan, P., & Kuo, S. (2019). Performance monitoring unit sharing guide. *Intel White Paper, http://software. intel. com/file/30388,(30388-PMU-Sharing-Guidelines. pdf)*.
10. Banitalebi Dehkordi, A., Soltanaghaei, M., & Boroujeni, F. Z. (2021). The DDoS attacks detection through machine learning and statistical methods in SDN. *The Journal of Supercomputing*, *77*, 2383-2415.
11. Fu, Y., Duan, X., Wang, K., & Li, B. (2022). Low-rate Denial of Service attack detection method based on time-frequency characteristics. *Journal of Cloud Computing*, *11*(1), 31.
12. Fouladi, R. F., Ermiş, O., & Anarim, E. (2020). A DDoS attack detection and defense scheme using time-series analysis for SDN. *Journal of Information Security and Applications*, *54*, 102587.
13. Dong, S., & Sarem, M. (2019). DDoS attack detection method based on improved KNN with the degree of DDoS attack in software-defined networks. *IEEE Access*, *8*, 5039-5048.
14. Lysenko, S., Bobrovnikova, K., Matiukh, S., Hurman, I., & Savenko, O. (2020). Detection of the botnets' low-rate DDoS attacks based on self-similarity. *International Journal of Electrical and Computer Engineering*, *10*(4), 3651-3659.
15. Aysa, M. H., Ibrahim, A. A., & Mohammed, A. H. (2020, October). Iot ddos attack detection using machine learning. In *2020 4th International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT)* (pp. 1-7). IEEE.
16. AbdelAzim, N. M., Fahmy, S. F., Sobh, M. A., & Eldin, A. M. B. (2021). A hybrid entropy-based DoS attacks detection system for software defined networks (SDN): A proposed trust mechanism. *Egyptian Informatics Journal*, *22*(1), 85-90.
17. Cheng, H., Liu, J., Xu, T., Ren, B., Mao, J., & Zhang, W. (2020). Machine learning based low-rate DDoS attack detection for SDN enabled IoT networks. *International Journal of Sensor Networks*, *34*(1), 56-69.
18. Mubarakali, A., Srinivasan, K., Mukhalid, R., Jaganathan, S. C., & Marina, N. (2020). Security challenges in internet of things: Distributed denial of service attack detection using support vector machine‐based expert systems. *Computational Intelligence*, *36*(4), 1580-1592.
19. Mubarakali, A., Srinivasan, K., Mukhalid, R., Jaganathan, S. C., & Marina, N. (2020). Security challenges in internet of things: Distributed denial of service attack detection using support vector machine‐based expert systems. *Computational Intelligence*, *36*(4), 1580-1592.
20. Gaurav, A., Gupta, B. B., & Panigrahi, P. K. (2022). A novel approach for DDoS attacks detection in COVID-19 scenario for small entrepreneurs. *Technological Forecasting and Social Change*, *177*, 121554.
21. Guide, P. (2011). Intel® 64 and ia-32 architectures software developer's manual. *Volume 3B: System programming Guide, Part*, *2*
22. Shah, S., Gandhi, D., & Kothari, J. (2020, November). Machine learning based Synthetic Data Generation using Iterative Regression Analysis. In *2020 4th International Conference on Electronics, Communication and Aerospace Technology (ICECA)* (pp. 1093-1100). IEEE.
23. Villegas, J., Cobos, C., Mendoza, M., & Herrera-Viedma, E. (2018). Feature selection using sampling with replacement, covering arrays and rule-induction techniques to aid polarity detection in twitter sentiment analysis. In *Advances in Artificial Intelligence-IBERAMIA 2018: 16th Ibero-American Conference on AI, Trujillo, Peru, November 13-16, 2018, Proceedings 16* (pp. 467-480). Springer International Publishing.
24. Schneider, M. (2016, May). Probability inequalities for kernel embeddings in sampling without replacement. In *Artificial Intelligence and Statistics* (pp. 66-74). PMLR.
25. <https://docs.python.org/ko/3/library/random.html>
26. Ting, D. (2021). Simple, optimal algorithms for random sampling without replacement. *arXiv preprint arXiv:2104.05091*.
27. Matsumoto, M., & Nishimura, T. (1998). Mersenne twister: a 623-dimensionally equidistributed uniform pseudo-random number generator. *ACM Transactions on Modeling and Computer Simulation (TOMACS)*, *8*(1), 3-30.
28. Edwards, J. R. (2007). Polynomial regression and response surface methodology. *Perspectives on organizational fit*, 361-372.
29. Korkmaz, M. (2021). A study over the general formula of regression sum of squares in multiple linear regression. *Numerical Methods for Partial Differential Equations*, *37*(1), 406-421.
30. Higham, N. J. (2011). Gaussian elimination. *Wiley Interdisciplinary Reviews: Computational Statistics*, *3*(3), 230-238.
31. Chai, T., & Draxler, R. R. (2014). Root mean square error (RMSE) or mean absolute error (MAE). *Geoscientific model development discussions*, *7*(1), 1525-1534.
32. Miles, J. (2005). R‐squared, adjusted R‐squared. *Encyclopedia of statistics in behavioral science*.
33. Kopytov, A. (2004). Sysbench: a system performance benchmark. *http://sysbench. sourceforge. net/*.
34. [perf-diff(1) - Linux manual page (man7.org)](https://man7.org/linux/man-pages/man1/perf-diff.1.html)
35. [perf-record(1) - Linux manual page (man7.org)](https://man7.org/linux/man-pages/man1/perf-record.1.html)
36. [Linux perf Examples (brendangregg.com)](https://www.brendangregg.com/perf.html)
37. Shahapure, K. R., & Nicholas, C. (2020, October). Cluster quality analysis using silhouette score. In *2020 IEEE 7th international conference on data science and advanced analytics (DSAA)* (pp. 747-748). IEEE.
38. Hartigan, J. A., & Wong, M. A. (1979). Algorithm AS 136: A k-means clustering algorithm. *Journal of the royal statistical society. series c (applied statistics)*, *28*(1), 100-108.
39. [sklearn.cluster.KMeans — scikit-learn 1.3.0 documentation](https://scikit-learn.org/stable/modules/generated/sklearn.cluster.KMeans.html)
40. Linero-Bas, A., & Nieves-Roldán, D. (2021). A generalization of the monotone convergence theorem. *Mediterranean Journal of Mathematics*, *18*(4), 158.
41. Teismann, H. (2013). Toward a more complete list of completeness axioms. *The American Mathematical Monthly*, *120*(2), 99-114.
42. Kodinariya, T. M., & Makwana, P. R. (2013). Review on determining number of Cluster in K-Means Clustering. *International Journal*, *1*(6), 90-95.
43. Saputra, D. M., Saputra, D., & Oswari, L. D. (2020, May). Effect of distance metrics in determining k-value in k-means clustering using elbow and silhouette method. In *Sriwijaya International Conference on Information Technology and Its Applications (SICONIAN 2019)* (pp. 341-346). Atlantis Press.
44. Obilor, E. I., & Amadi, E. C. (2018). Test for significance of Pearson’s correlation coefficient. *International Journal of Innovative Mathematics, Statistics & Energy Policies*, *6*(1), 11-23.
45. Myers, L., & Sirois, M. J. (2004). Spearman correlation coefficients, differences between. *Encyclopedia of statistical sciences*, *12*.
46. Prematunga, R. K. (2012). Correlational analysis. *Australian Critical Care*, *25*(3), 195-199.
47. Bishara, A. J., & Hittner, J. B. (2012). Testing the significance of a correlation with nonnormal data: comparison of Pearson, Spearman, transformation, and resampling approaches. *Psychological methods*, *17*(3), 399.
48. [Keras: Deep Learning for humans](https://keras.io/)
49. <http://scikit-learn.org>
50. Priya, S. S., Sivaram, M., Yuvaraj, D., & Jayanthiladevi, A. (2020, March). Machine learning based DDoS detection. In *2020 International Conference on Emerging Smart Computing and Informatics (ESCI)* (pp. 234-237). IEEE.
51. Kim, Y., Hakak, S., & Ghorbani, A. (2023). Smart grid security: Attacks and defence techniques. *IET Smart Grid*, *6*(2), 103-123.
52. O’Neil, L. R., Carroll, T. E., Abdelhadi, E. M., Watson, M. D., Hammer, C. L., & Psarakis, M. B. Sample Cybersecurity Clauses for EV Charging Infrastructure Procurements.
53. Chavali, S., Cheema, H., Delgado, R., Nolan, E., Ibrahem, M. I., & Fouda, M. M. (2023, April). A Review of Privacy-Preserving Authentication Schemes for Future Internet of Vehicles. In *2023 IEEE 12th International Conference on Communication Systems and Network Technologies (CSNT)* (pp. 689-694). IEEE.
54. Roman, L. F., & Gondim, P. R. (2023). Trust Management and Authentication Protocol for CWD-WPT Charging Stations.
55. Hou, W., Sun, Y., Li, D., Guan, Z., & Liu, J. (2023). Lightweight and Privacy-Preserving Charging Reservation Authentication Protocol for 5G-V2G. *IEEE Transactions on Vehicular Technology*.
56. Parameswarath, R. P., Gope, P., & Sikdar, B. (2023). Privacy-Preserving User-Centric Authentication Protocol for IoT-Enabled Vehicular Charging System Using Decentralized Identity. *IEEE Internet of Things Magazine*, *6*(1), 70-75.
57. Reddy, A. G., Babu, P. R., Odelu, V., Wang, L., & Kumar, S. A. (2023). V2G-Auth: Lightweight Authentication and Key Agreement Protocol for V2G Environment leveraging Physically Unclonable Functions. *IEEE Transactions on Industrial Cyber-Physical Systems*.
58. Parameswarath, R. P., Gope, P., & Sikdar, B. (2023). A Privacy-Preserving Authenticated Key Exchange Protocol for V2G Communications Using SSI. *IEEE Transactions on Vehicular Technology*.
59. Wanga, B., Guob, X., & Zhangc, S. A Conditional Privacy-Preserving Authentication Scheme for Electricity Transaction in V2G Network.
60. Haugneland, P., Lorentzen, E., Bu, C., & Hauge, E. (2017, October). Put a price on carbon to fund EV incentives–Norwegian EV policy success. In *EVS30 Symposium. Stuttgart, Germany, EN*.
61. Liu, Y., Zhu, J., Sang, Y., Sahraei-Ardakani, M., Jing, T., Zhao, Y., & Zheng, Y. (2023). An aggregator-based dynamic pricing mechanism and optimal scheduling scheme for the electric vehicle charging. *Frontiers in Energy Research*, *10*, 1037253.
62. Mwasilu, F., Justo, J. J., Kim, E. K., Do, T. D., & Jung, J. W. (2014). Electric vehicles and smart grid interaction: A review on vehicle to grid and renewable energy sources integration. *Renewable and sustainable energy reviews*, *34*, 501-516.
63. Sayed, M. A., Atallah, R., Assi, C., & Debbabi, M. (2022). Electric vehicle attack impact on power grid operation. *International Journal of Electrical Power & Energy Systems*, *137*, 107784.
64. Basnet, M., & Ali, M. H. (2022, December). WCGAN-Based Cyber-Attacks Detection System in the EV Charging Infrastructure. In *2022 4th International Conference on Smart Power & Internet Energy Systems (SPIES)* (pp. 1761-1766). IEEE.
65. Li, S., Cao, Y., Liu, S., Lai, Y., Zhu, Y., & Ahmad, N. Hda-Ids: A Hybrid Dos Attacks Intrusion Detection System for Ev Charging Infrastructure. *Available at SSRN 4355728*.
66. Ring, M., Wunderlich, S., Scheuring, D., Landes, D., & Hotho, A. (2019). A survey of network-based intrusion detection data sets. Computers & Security, 86, 147-167.
67. Hekmati, A., Grippo, E., & Krishnamachari, B. (2021, November). Large-scale urban iot activity data for ddos attack emulation. In *Proceedings of the 19th ACM Conference on Embedded Networked Sensor Systems* (pp. 560-564).