**Appendix A2. The Output of the PART Classifier**

Before selecting the final detection model, the PART classifier is used to extract the second detection ruleset using the two training datasets described in Section 4 as classifier input, as illustrated in Fig. 14. Thus, there are two outputs.

1. **The mixed dataset output for the PART classifier is:**

|  |  |  |
| --- | --- | --- |
| === Run information === | | |
| Scheme | : | weka.classifiers.rules.PART -M 2 -C 0.25 -Q 1 |
| Relation | : | mix 100-weka.filters.unsupervised.attribute.Remove-R1 |
| Instances | : | 45202 |
| Attributes | : | 11 |
|  |  | NO\_Distinct\_Destination |
|  |  | Arg\_TTL |
|  |  | NO\_Distinct\_TTL |
|  |  | NO\_Distinct\_Packet |
|  |  | No\_suc\_resp |
|  |  | No\_error\_resp |
|  |  | Avg\_domain\_ent |
|  |  | Ratio\_suc\_resp |
|  |  | rand\_query |
|  |  | number\_record\_type |
|  |  | Class |
| Test mode | : | 10-fold cross-validation |

=== Classifier model (full training set) ===

PART decision list

------------------

|  |  |  |
| --- | --- | --- |
| NO\_Distinct\_TTL <= 1 AND | | |
| NO\_Distinct\_Packet > 1 AND | | |
| Ratio\_suc\_resp <= 0.857143 AND | | |
| No\_error\_resp > 5: attack (43282.0) | | |
| NO\_Distinct\_TTL > 2 AND | | |
| No\_error\_resp <= 1 AND | | |
| NO\_Distinct\_TTL > 3: normal (279.0/2.0) | | |
| No\_error\_resp > 0 AND | | |
| NO\_Distinct\_TTL <= 2 AND | | |
| No\_suc\_resp > 2: attack (397.0) | | |
| NO\_Distinct\_TTL <= 1 AND | | |
| number\_record\_type <= 1 AND | | |
| Arg\_TTL <= 294.716667 AND | | |
| Ratio\_suc\_resp <= 0.75 AND | | |
| No\_error\_resp > 0 AND | | |
| rand\_query <= 1.247556: attack (290.0) | | |
| NO\_Distinct\_TTL <= 1 AND | | |
| number\_record\_type <= 1 AND | | |
| Arg\_TTL <= 294.716667 AND | | |
| No\_suc\_resp > 0: attack (283.0/1.0) | | |
| NO\_Distinct\_TTL > 1 AND | | |
| No\_suc\_resp <= 4 AND | | |
| Ratio\_suc\_resp > 0.533333: normal (239.0) | | |
| NO\_Distinct\_Destination > 2 AND | | |
| Ratio\_suc\_resp <= 0.487179: attack (104.0) | | |
| number\_record\_type <= 2 AND | | |
| No\_error\_resp <= 7 AND | | |
| Avg\_domain\_ent > 3.324112 AND | | |
| number\_record\_type > 0 AND | | |
| No\_suc\_resp > 3 AND | | |
| NO\_Distinct\_TTL <= 3 AND | | |
| No\_error\_resp <= 1 AND | | |
| Avg\_domain\_ent > 3.440818: attack (42.0) | | |
| number\_record\_type > 2: attack (42.0) | | |
| No\_error\_resp <= 7 AND | | |
| number\_record\_type <= 0 AND | | |
| Avg\_domain\_ent > 3.441374: attack (30.0/1.0) | | |
| No\_error\_resp > 7: attack (28.0/1.0) | | |
| Arg\_TTL <= 21600 AND | | |
| NO\_Distinct\_Packet > 3 AND | | |
| Arg\_TTL <= 7147: normal (27.0/1.0) | | |
| No\_suc\_resp <= 1 AND | | |
| NO\_Distinct\_TTL > 0: normal (22.0) | | |
| Arg\_TTL > 449.875 AND | | |
| number\_record\_type > 1 AND | | |
| Avg\_domain\_ent > 2.805876 AND | | |
| NO\_Distinct\_TTL <= 1: attack (24.0) | | |
| NO\_Distinct\_Packet <= 3 AND | | |
| No\_suc\_resp > 7 AND | | |
| Avg\_domain\_ent > 2.831039 AND | | |
| NO\_Distinct\_Destination > 1: attack (8.0) | | |
| NO\_Distinct\_Packet <= 3 AND | | |
| No\_error\_resp > 0 AND | | |
| NO\_Distinct\_Destination <= 1: attack (12.0) | | |
| NO\_Distinct\_Packet <= 3 AND | | |
| No\_error\_resp <= 1 AND | | |
| NO\_Distinct\_TTL > 0 AND | | |
| No\_suc\_resp <= 3: normal (22.0) | | |
| NO\_Distinct\_Packet <= 3 AND | | |
| No\_error\_resp <= 1 AND | | |
| rand\_query <= 1.666056 AND | | |
| NO\_Distinct\_Destination <= 1 AND | | |
| Ratio\_suc\_resp <= 0.125: normal (21.0/6.0) | | |
| Avg\_domain\_ent > 2.893186 AND | | |
| No\_error\_resp <= 2 AND | | |
| No\_error\_resp <= 1 AND | | |
| NO\_Distinct\_Destination <= 1 AND | | |
| NO\_Distinct\_TTL <= 2 AND | | |
| Ratio\_suc\_resp <= 1.054054 AND | | |
| NO\_Distinct\_Packet <= 2: attack (16.0/2.0) | | |
| NO\_Distinct\_Packet <= 3 AND | | |
| NO\_Distinct\_Packet > 1 AND | | |
| Avg\_domain\_ent <= 3.361146 AND | | |
| Arg\_TTL <= 1969.230769: normal (17.0) | | |
| Ratio\_suc\_resp <= 1.1 | : | attack (14.0) |
|  | : | normal (3.0/1.0) |
|  | | |
| Number of Rules | : | 22 |
|  | | |
|  | | |
| Time taken to build model |  | 0.8 seconds |

**2. The NIMS dataset output for the PART classifier is:**

|  |  |  |
| --- | --- | --- |
| === Run information === | | |
| Scheme | : | weka.classifiers.rules.PART -M 2 -C 0.25 -Q 1 |
| Relation | : | nims 100 |
| Instances | : | 44677 |
| Attributes | : | 12 |
|  |  | Source\_IP |
|  |  | NO\_Distinct\_Destination |
|  |  | Arg\_TTL |
|  |  | NO\_Distinct\_TTL |
|  |  | NO\_Distinct\_Packet |
|  |  | No\_suc\_resp |
|  |  | No\_error\_resp |
|  |  | Avg\_domain\_ent |
|  |  | Ratio\_suc\_resp |
|  |  | rand\_query |
|  |  | number\_record\_type |
|  |  | Class |
| Test mode | : | 10-fold cross-validation |

=== Classifier model (full training set) ===

PART decision list

------------------

|  |  |  |
| --- | --- | --- |
| NO\_Distinct\_TTL <= 2 AND | | |
| Ratio\_suc\_resp <= 0.727273 AND | | |
| No\_error\_resp > 0: attack (44003.0) | | |
| NO\_Distinct\_TTL <= 3 AND | | |
| number\_record\_type <= 1: attack (405.0) | | |
| NO\_Distinct\_TTL > 3 AND | | |
| No\_error\_resp <= 10 AND | | |
| NO\_Distinct\_Packet > 4: normal (52.0) | | |
| No\_error\_resp > 1: attack (69.0) | | |
| Avg\_domain\_ent > 3.307406 AND | | |
| NO\_Distinct\_Destination <= 1 AND | | |
| NO\_Distinct\_Packet <= 2: attack (38.0/1.0) | | |
| Avg\_domain\_ent <= 3.440818 AND | | |
| NO\_Distinct\_Packet > 3 AND | | |
| Avg\_domain\_ent <= 3.305419: normal (24.0) | | |
| Avg\_domain\_ent > 2.828196 AND | | |
| No\_suc\_resp > 3 AND | | |
| Arg\_TTL > 576: attack (47.0/1.0) | | |
| NO\_Distinct\_TTL > 0 AND | | |
| Avg\_domain\_ent <= 3.451193 AND | | |
| NO\_Distinct\_Destination <= 2 AND | | |
| rand\_query <= 1.501614: normal (16.0) | | |
| NO\_Distinct\_TTL <= 1: attack (17.0/1.0) | | |
|  | : | normal (6.0/1.0) |
|  | | |
| Number of Rules | : | 10 |
|  | | |
|  | | |
| Time taken to build model | : | * 1. seconds |